
3 1761 07548295 0





LEÇONS

SUR LA

THÉORIE DES NOMBRES.

LEÇONS

SUR LA

THÉORIE DES NOMBRES

(MODULES. ENTIERS ALGÉBRIQUES.
RÉDUCTION CONTINUELLE.)

PROFESSÉES AU COLLÈGE DE FRANCE

PAR

A. CHÂTELET,

ANCIEN ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE,
CHARGÉ DE COURS A LA FACULTÉ DES SCIENCES DE TOULOUSE.



PARIS,
GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE
DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.

—

1913

A

LA MÉMOIRE DE MON PÈRE.

PRÉFACE.

Ces leçons ont été, à quelques additions près, professées au Collège de France, pendant le deuxième semestre de l'année 1911-1912, pour le cours de la Fondation Peccot. J'ai essayé d'en faire une sorte d'introduction à l'étude des notions et théories nouvelles introduites depuis une soixantaine d'années en Arithmétique supérieure, un peu comme conséquence des travaux de Gauss et sous l'influence des idées de Galois et d'Hermite. Ce Livre peut ainsi être considéré comme un complément aux Traités français actuels de Théorie des Nombres (*Algèbre* de Serret, *Leçons* de J. Tannery, rédigées par MM. Borel et Drach, *Traité* de M. Cahen, etc.), Traités qui sont limités aux théories de Legendre, Jacobi et Gauss.

Pour ne pas allonger outre mesure l'exposition, je n'ai pas repris toute chose à son début, et n'ai pas essayé de constituer une science isolée indépendante de tout concept d'Algèbre et d'Analyse. Cependant, je n'ai fait appel qu'à des résultats mathématiques préalables assez élémentaires : les premières notions d'Arithmétique, quelques principes de la théorie des systèmes d'équations linéaires et des équations algébriques (qui font partie du programme actuel de la classe de Mathématiques spéciales), quelques définitions de la théorie des ensembles de points et des intégrales multiples (qu'on trouve dans les Traités classiques d'Analyse).

J'ai rassemblé, dans le premier Chapitre, d'autres notions d'Algèbre et d'Analyse, moins universellement adoptées; la notation des Tableaux, exposée surtout d'après les travaux de Laguerre

et de M. Jordan; le langage géométrique (espace à n dimensions); la généralisation de la notion de distance indiquée par M. Minkowski et le volume d'un corps convexe dans l'espace à n dimensions.

Les quatre Chapitres suivants sont consacrés à l'exposition de la théorie des modules et de ses applications. C'est à M. Dedekind qu'on doit une des premières expositions méthodiques de cette théorie, déjà en germe dans les travaux d'Hermite. Elle m'a permis de relier un assez grand nombre de résultats, en apparence assez éloignés : divisibilité des entiers ordinaires, approximations des irrationnelles, équations diophantiques, théorie des entiers complexes algébriques, périodes des fonctions, etc. On y trouvera notamment plusieurs résultats arithmétiques énoncés et établis isolément par Hermite, surtout en vue de la transformation des fonctions abéliennes.

Dans les deux derniers Chapitres a été exposée, d'après les idées d'Hermite, la célèbre méthode de la réduction continuelle et son application toute naturelle aux formes décomposables et aux corps algébriques (unités, corps d'un discriminant donné, classes d'idéaux). J'ai indiqué à ce sujet l'énoncé et la démonstration des deux importants théorèmes de la *Geometrie der Zahlen* de M. Minkowski, théorèmes qui complètent, en permettant de l'étendre, la méthode d'Hermite.

Les Chapitres IV, V et VII, plus spécialement consacrés aux nombres algébriques, constituent les premiers éléments de la théorie des entiers complexes d'un corps et de leur arithmétique. On sait que cette théorie, qui a pris en Allemagne une grande extension, a été laissée en France, depuis Hermite, dans un oubli assez curieux; à part deux traductions récentes (*Introduction* de M. Sommer, traduit par M. Lévy, et *Rapport* de M. Hilbert, traduit par MM. Lévy et Got), un article original de M. Dedekind (*Bulletin des Sciences mathématiques*) et un court opuscule de

M. Laurent (Paris, 1904), il n'existe, à ma connaissance, aucun Exposé français sur la question.

J'ai ajouté trois Notes à ce Livre; dans la première, j'ai exposé l'application de la théorie des modules de points aux périodes des fonctions, ce qui m'a permis d'indiquer, d'après M. Esclangon, la définition et quelques propriétés arithmétiques des *fonctions quasi-périodiques*. Dans la deuxième, on trouvera une application numérique, à un corps quadratique, des définitions et principes énoncés pour les corps algébriques généraux. C'est un peu plus qu'un exemple numérique; j'ai indiqué succinctement, à propos du cas particulier considéré, des procédés de recherche applicables à tous les corps quadratiques. J'espère que ceci compensera un peu l'absence d'une théorie particulière de ces corps, le cadre forcément restreint de ces leçons ne m'ayant pas permis de l'y introduire. Enfin, dans la troisième Note, on trouvera quelques notions complémentaires sur l'Arithmétique des idéaux.

Tel qu'il est, ce petit Livre n'a pas la prétention d'être un Mémoire original, et les propriétés qui y sont indiquées ont été déjà publiées; sur bien des points, je n'ai pas essayé d'atteindre les limites de la science actuelle, renvoyant le lecteur désireux d'aller plus loin à des Traités spéciaux ou à des Mémoires originaux. Par contre, je ne me suis pas astreint à exposer les travaux des divers auteurs sous la forme précise qu'ils avaient adoptée primitivement (j'ai ainsi modifié quelque peu la méthode de réduction continuelle d'Hermite, l'exposition de la théorie des modules de Dedekind, etc.); je n'ai pas voulu non plus me rattacher à une école déterminée et, dans la théorie des entiers algébriques, par exemple, j'ai emprunté indifféremment des procédés aux méthodes d'exposition de Dedekind ou de Kronecker, aux travaux de Minkowski, Hurwitz, etc. J'ai surtout essayé de faire une œuvre homogène et de mettre le plus possible en évidence les relations mutuelles des faits et ce qui m'a paru leur véritable raison d'être. Il m'est arrivé

ainsi de modifier souvent des démonstrations ou des énoncés, et il m'eût été difficile de renvoyer toujours avec précision à un Mémoire original. Je prie les lecteurs désireux d'avoir des renseignements bibliographiques plus développés de se reporter : pour l'étude des nombres entiers proprement dits (divisibilité et équations diophantiques) à l'*Essai sur la Théorie des Nombres*, de T.-J. Stieltjes; pour les nombres algébriques, à l'abondante bibliographie du *Rapport* de M. Hilbert (*Jahrb. der deuts. math. Ver.*, 1897) et du *Rapport* plus récent de M. Fueter (*Ibid.*, 1911); enfin, d'une façon générale, à l'*Encyclopédie des Sciences mathématiques*, éditions allemande et française, à laquelle j'ai fait d'ailleurs de nombreux renvois dans le cours du Livre. Je dois signaler que j'ai fait de très larges emprunts aux Œuvres d'Hermite; j'ai également beaucoup emprunté à M. Minkowski qui, sur de nombreux points, a été le continuateur du grand géomètre français.

C'est sur la demande de mes auditeurs du Collège de France que j'ai songé à publier ces Leçons; l'un d'eux, M. Vidil, élève de 2e année à l'École Normale supérieure, a bien voulu rédiger ses propres notes à cette intention. J'en ai tiré un très grand profit, et je suis heureux de lui en exprimer ici toute ma reconnaissance.

Je tiens aussi à remercier M. Gauthier-Villars, qui a bien voulu se charger de l'impression et de l'édition de ce petit Livre. Il m'a rendu ainsi un grand service, je serais heureux si j'avais la certitude qu'il en a rendu en même temps un petit à la Science française.

Toulouse, 2 mars 1913.

LEÇONS

SUR LA

THÉORIE DES NOMBRES.

CHAPITRE I.

INTRODUCTION ALGÉBRIQUE.

Les formes et substitutions linéaires.

Il y a souvent lieu, en Arithmétique supérieure, d'utiliser des résultats de l'algèbre (ou plus exactement du calcul algébrique), notamment de la théorie des formes et substitutions linéaires. Nous allons d'abord rappeler brièvement quelques principes de cette théorie et indiquer en même temps les notations que nous utiliserons dans la suite.

Un système de n formes linéaires indépendantes de n variables $x_1, x_2, \ldots, x_n$

$$(1) \qquad \xi_i = a_1^i x_1 + a_2^i x_2 + \ldots + a_n^i x_n \qquad (i = 1, 2, \ldots, n),$$

ou encore la substitution représentée par les mêmes formules (ξ anciennes variables, x nouvelles), est complètement déterminé quand on se donne les coefficients; pour rappeler leur place respective dans les formes, on a coutume de les ranger en un tableau carré

$$(2) \qquad \begin{Vmatrix} a_1^1 & a_1^2 & \ldots & a_1^n \\ a_2^1 & a_2^2 & \ldots & a_2^n \\ \ldots & \ldots & \ldots & \ldots \\ a_n^1 & a_n^2 & \ldots & a_n^n \end{Vmatrix}$$

(les coefficients de la $i^{\text{ième}}$ *forme* occupant la $i^{\text{ième}}$ *colonne*).

Il y a souvent avantage à raisonner directement sur ce tableau, auquel on attribue ainsi une existence indépendante. C'est ce qu'ont fait de nombreux algébristes et arithméticiens, et il nous suffira de citer l'exemple d'Hermite (dans la transformation des fonctions abéliennes) et de Cayley [1]. Nous désignerons donc un tel système de n^2 nombres par une seule lettre A et nous supposerons, sauf mention du contraire, que le déterminant $\Delta(A)$ formé par les n^2 nombres n'est pas nul; le tableau sera dit alors d'*ordre* ou de *rang n*. Le système de formes, la substitution (1) seront dits *associés* au tableau; leur donnée entraîne celle de A et réciproquement [pour cette réciproque, on conçoit la nécessité de l'hypothèse $\Delta(A) \neq 0$].

La *somme* de deux tableaux de même ordre est un tableau de même ordre, où chaque terme est la somme des termes de même rang dans les deux premiers. Ainsi

$$\begin{Vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{Vmatrix} + \begin{Vmatrix} a_1 & b_1 & c_1 \\ a'_1 & b'_1 & c'_1 \\ a''_1 & b''_1 & c''_1 \end{Vmatrix} = \begin{Vmatrix} a + a_1 & b + b_1 & c + c_1 \\ a' + a'_1 & b' + b'_1 & c' + c'_1 \\ a'' + a''_1 & b'' + b''_1 & c'' + c''_1 \end{Vmatrix}.$$

Cette opération est *associative* et *commutative*, mais il se peut que le résultat ne soit pas un tableau de rang n, son déterminant pouvant être nul. Nous verrons ultérieurement des applications de cette notion.

Le *produit* de deux tableaux de même ordre $A \times B$ est un tableau de même ordre, où le terme a_i^j s'obtient en faisant la somme des produits des termes de la ligne de rang i du premier tableau A par les termes correspondants de la colonne de rang j du second B. Ainsi

$$\begin{Vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{Vmatrix} \times \begin{Vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{Vmatrix}$$

$$= \begin{Vmatrix} a\alpha + b\alpha' + c\alpha'' & a\beta + b\beta' + c\beta'' & a\gamma + b\gamma' + c\gamma'' \\ a'\alpha + b'\alpha' + c'\alpha'' & a'\beta + b'\beta' + c'\beta'' & a'\gamma + b'\gamma' + c'\gamma'' \\ a''\alpha + b''\alpha' + c''\alpha'' & a''\beta + b''\beta' + c''\beta'' & a''\gamma + b''\gamma' + c''\gamma'' \end{Vmatrix}.$$

---

(1) On peut même considérer de tels systèmes comme généralisant les nombres ordinaires et constituant des nombres *complexes* (*voir* là-dessus l'article de MM. Study et Cartan, *Encyclopédie*, t. I, vol. I, fasc. 3).

Cette opération ([1]) est évidemment *associative*

$$A \times (B \times C) = (A \times B) \times C;$$

elle est aussi *distributive* par rapport à l'addition

$$A \times (B + C) = A \times B + A \times C,$$
$$(B + C) \times A = B \times A + C \times A.$$

D'autre part, la règle pour former les termes du produit coïncide avec l'une des règles habituellement indiquées pour former le produit de deux déterminants. Donc

$$\Delta(A \times B) = \Delta(A) \times \Delta(B).$$

Mais cette opération n'est pas, en général, *commutative;* $A \times B$ n'est pas nécessairement égal à $B \times A$, et il y a lieu de distinguer le produit à *droite* et le produit à *gauche* par un tableau.

On remarquera, et ceci donne une raison d'être de la définition précédente, que la substitution associée au tableau $A \times B$ est le produit des substitutions associées à chacun des facteurs, entendant par là que c'est le résultat obtenu en faisant d'abord la substitution B, puis, sur les nouvelles variables ainsi obtenues, la substitution A. D'autre part, le système de formes associé à $A \times B$ s'obtient en faisant la substitution A sur les variables du système associé à B.

Un tableau est dit *système simple* et désigné par $[m]$ quand tous ses termes sont nuls, à l'exception de ceux de la diagonale principale ([2]), ceux-ci étant tous égaux à m. On obtient manifestement $[m] \times A$ ou $A \times [m]$, ou simplement mA, en multipliant tous les termes de A par m. Les calculs entre systèmes simples se réduisent aux calculs sur les nombres qui les constituent :

$$[m] + [p] = [m + p],$$
$$[m] \times [p] = [mp].$$

Le système simple [1] joue le rôle de l'unité, car c'est le seul

([1]) On pourrait adopter une définition en multipliant colonnes par lignes. De même, on aurait pu établir autrement la correspondance entre tableau et substitution. La nécessité de fixer ces conventions est une des raisons de cette introduction.

([2]) Cette notation suppose, bien entendu, connu l'ordre du tableau.

tableau vérifiant les équations

$$X \times A = A \quad \text{ou} \quad A \times X = A \quad [\Delta(A) \neq 0].$$

Pour cette raison, nous appellerons *tableau inverse* de A le tableau A^{-1} défini par l'une des égalités

$$A \times A^{-1} = [1] \quad \text{ou} \quad A^{-1} \times A = [1].$$

A cet inverse est associée la *substitution inverse* de celle associée à A (qui fait passer des nouvelles variables aux anciennes); il est donc *unique* (¹) et vérifie les deux égalités. On l'obtiendra, par exemple, en résolvant les équations (1) par rapport aux x et en prenant les coefficients des formes en ξ ainsi obtenues. On peut encore dire que ses termes sont ceux du *déterminant adjoint* de $\Delta(A)$, divisés par le nombre $\Delta(A)$, et après permutation de lignes et colonnes. Le déterminant de $[1]$ étant 1, celui de A^{-1} est $\frac{1}{\Delta(A)}$; l'inverse du système simple $[m]$ est $\left[\frac{1}{m}\right]$. Enfin, l'inverse d'un produit s'obtient par la règle simple

$$(A \times B \times \ldots \times K \times L)^{-1} = L^{-1} \times K^{-1} \times \ldots \times B^{-1} \times A^{-1};$$

puisque l'inverse est unique, il suffit de faire la vérification, ce qui est immédiat.

Donnons, en terminant, quelques notions sur les *matrices*. Nous appellerons ainsi un tableau rectangulaire ou carré de nombres, d'où l'on peut déduire, par suppression de lignes et de colonnes, des tableaux carrés. On pourra distinguer dans une matrice : le *type* (m, p), m lignes et p colonnes; le *rang* r, ordre du tableau d'ordre le plus élevé (à déterminant non nul) qu'on peut en déduire. Le rang est au plus égal au plus petit des deux nombres m, p. Pour qu'on puisse étendre à deux matrices la définition de la somme, il faut et il suffit qu'elles soient de même type. Pour étendre la définition du produit, il suffit que le nombre de colonnes de la première (matrice de gauche) soit égal au

(¹) On pourrait encore démontrer cette unicité et l'équivalence des deux équations de définition, soit en se servant des n^2 équations linéaires par rapport aux termes de A^{-1} qui traduisent cette définition, soit en utilisant l'unicité de la solution de $XA = A$ et de $AX = A$, et les propriétés du produit. Cette dernière méthode aurait un intérêt au point de vue du calcul symbolique en général.

nombre de lignes de la deuxième : $p = m'$. L'extension de la règle est alors immédiate, on obtient une matrice du type (m, p'). La multiplication ainsi définie est encore associative ; on le vérifie aisément, c'est sa seule propriété utilisée, en général.

Cette définition du produit permet, par exemple, de représenter la substitution (1) par l'égalité

$$\| \xi_1 \quad \xi_2 \quad \dots \quad \xi_n \| = \| x_1 \quad x_2 \quad \dots \quad x_n \| \times A.$$

A désigne le tableau (2) associé à la substitution. Nous écrirons les matrices et les tableaux, encadrées de deux doubles barres verticales, pour les distinguer des déterminants qui sont des *nombres*.

Ensembles abéliens de tableaux.

On peut se proposer de former des ensembles de tableaux où la *multiplication soit commutative*. La recherche de tous ces ensembles, que nous appellerons, pour abréger, *abéliens* [1], est un problème compliqué ; je me contenterai d'indiquer ici une catégorie très étendue de tels ensembles. Une première solution nous serait donnée par l'ensemble des systèmes simples ; une autre, plus générale, par les tableaux où tous les termes, sauf ceux de la diagonale principale, sont nuls, mais les termes non nuls n'étant plus nécessairement égaux. Par exemple,

$$[\alpha_1, \alpha_2, \dots, \alpha_n] = \left\| \begin{matrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ . & .. & \dots & . \\ 0 & 0 & \dots & \alpha_n \end{matrix} \right\|.$$

La notation adoptée est évidente ; nous dirons qu'un tel tableau est *élémentaire* ou *canonique*. Les règles de calcul sont aussi manifestes :

$$[\alpha_1, \alpha_2, \dots, \alpha_n] + [\beta_1, \beta_2, \dots, \beta_n] = [\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n],$$

$$[\alpha_1, \alpha_2, \dots, \alpha_n] \times [\beta_1, \beta_2, \dots, \beta_n] = [\alpha_1 \beta_1, \alpha_2 \beta_2, \dots, \alpha_n \beta_n],$$

$$[\alpha_1, \alpha_2, \dots, \alpha_n]^{-1} = \left[\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \dots, \frac{1}{\alpha_n} \right],$$

$$\Delta([\alpha_1, \alpha_2, \dots, \alpha_n]) = \alpha_1 \alpha_2 \dots \alpha_n.$$

---

(1) Suivant une locution habituelle en théorie des groupes.

La multiplication de deux tableaux canoniques est donc bien commutative; on peut aller plus loin. La définition même de la multiplication conduit à une règle simple pour le produit d'un tableau A par un tableau canonique E; il suffit de multiplier par α_i ($i = 1, 2, \ldots, n$) tous les termes de la *ligne* de rang i de A, si le produit est à *gauche* (E × A), et de la *colonne*, si le produit est à *droite* (A × E). En conséquence, si l'on suppose que les termes de E sont inégaux, pour que le tableau A soit permutable avec E, (AE = EA), il faut et il suffit qu'il soit canonique; l'égalité $\alpha_i a_i^j = \alpha_j a_i^j$ entraîne, en effet, $a_i^j = 0$ pour $i \neq j$. Donc, *si un ensemble abélien renferme un tableau canonique à termes distincts, cet ensemble ne renferme que des tableaux canoniques.*

Soit maintenant P un tableau déterminé $[\Delta(P) \neq 0]$ et E un tableau canonique quelconque. Les tableaux PEP^{-1} forment encore un ensemble abélien; c'est ce qui résulte des règles de calcul (conséquences des propriétés des opérations)

$$\begin{aligned}
PEP^{-1} + PE'P^{-1} &= P(EP^{-1} + E'P^{-1}) = P(E + E')P^{-1},\\
PEP^{-1} \times PE'P^{-1} &= P(E \times E')P^{-1},\\
(PEP^{-1})^{-1} &= (P^{-1})^{-1} \times E^{-1} \times P^{-1} = PE^{-1}P^{-1},\\
\Delta(PEP^{-1}) &= \Delta(P) \times \Delta(E) \times \Delta(P^{-1}) = \Delta(E).
\end{aligned}$$

Nous allons voir que c'est là le cas général des ensembles abéliens.

Montrons d'abord que tout tableau A peut être mis, en général, sous la forme précédente. C'est ce qui résulte d'un calcul bien connu (on le trouve notamment dans le *Traité des substitutions* de M. Jordan) sur la réduction d'une substitution à sa forme canonique. Voici comment, avec les notations adoptées, on peut se poser ce dernier problème. Soit la substitution associée à A,

$$\| x_1 \;\; x_2 \;\; \ldots \;\; x_n \| = \| y_1 \;\; y_2 \;\; \ldots \;\; y_n \| \cdot A;$$

peut-on considérer les x et les y comme provenant, par une même substitution P, des variables x' et y'

$$\begin{aligned}
\| x'_1 \;\; x'_2 \;\; \ldots \;\; x'_n \| &= \| x_1 \;\; x_2 \;\; \ldots \;\; x_n \| \cdot P,\\
\| y'_1 \;\; y'_2 \;\; \ldots \;\; y'_n \| &= \| y_1 \;\; y_2 \;\; \ldots \;\; y_n \| \cdot P,
\end{aligned}$$

les variables y' provenant des x' par une substitution cano-

nique (associée à un tableau canonique)

$$\| x'_1 \quad x'_2 \quad \ldots \quad x'_n \| = \| y'_1 \quad y'_2 \quad \ldots \quad y'_n \| \quad [\lambda_1, \lambda_2, \ldots, \lambda_n]$$

ou

$$x'_i = \lambda_i y'_i.$$

Le calcul est immédiat; en ayant égard à l'associativité des produits, le système précédent, qui doit être vérifié quels que soient les y, est équivalent à

$$(3) \qquad P \times [\lambda_1, \lambda_2, \ldots, \lambda_n] = A \times P.$$

Appelons a_i^j les termes de A supposés connus et α_i^j les termes de P à déterminer. L'égalité précédente se traduit par un système de n^2 équations en α et λ, qu'on peut grouper en n systèmes de n, obtenus respectivement en égalant les termes d'une même colonne dans le 1er et le 2e membre (les produits étant effectués) :

$$(3\ bis) \quad \left\{ \begin{array}{ll} a_i^1 \alpha_1^1 + a_i^2 \alpha_2^1 + \ldots + a_i^n \alpha_n^1 = \lambda_1 \alpha_i^1 & i = (1, 2, \ldots, n), \\ a_i^1 \alpha_1^2 + a_i^2 \alpha_2^2 + \ldots + a_i^n \alpha_n^2 = \lambda_2 \alpha_i^2 & \text{id.} \\ \ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots \\ a_i^1 \alpha_1^n + a_i^2 \alpha_2^n + \ldots + a_i^n \alpha_n^n = \lambda_n \alpha_i^n & \text{id.} \end{array} \right.$$

Considérons, par exemple, le premier système; il peut être envisagé comme formé d'équations homogènes en α_i^1 (termes de la première colonne de P). Son déterminant qui est alors une fonction de λ_1,

$$(4) \qquad \begin{vmatrix} a_1^1 - \lambda_1 & a_1^2 & \ldots & a_1^n \\ a_2^1 & a_2^2 - \lambda_1 & \ldots & a_2^n \\ \ldots & \ldots\ldots & \ldots & \ldots \\ a_n^1 & a_n^2 & \ldots & a_n^n - \lambda_1 \end{vmatrix}.$$

doit être nul. On raisonnerait de même pour le 2e, 3e, etc. système, en remplaçant seulement dans le déterminant λ_1 par λ_2, λ_3, ... Donc les λ doivent être racines de l'équation de degré n, connue sous le nom d'*équation en* λ *de* A, qu'on peut écrire, sous forme abrégée,

$$f(\lambda) \equiv \Delta(A - [\lambda]) = 0.$$

Cette équation ne saurait avoir de racine nulle, puisque $\Delta(A)$ n'est pas nul. Nous supposerons qu'elle n'a pas de racines mul-

tiples [1] : rangeons alors ses racines dans un ordre déterminé, soit $\lambda_1, \lambda_2, \ldots, \lambda_n$. L'une quelconque λ_k annule le déterminant ([illegible]), mais n'annule pas tous ses mineurs, sinon elle annulerait la dérivée de $f(\lambda)$ (somme des mineurs principaux). Donc, en transportant cette valeur dans le $k^{\text{ième}}$ système (3 *bis*), on trouve un système de valeurs pour $\alpha_1^k, \alpha_2^k, \ldots, \alpha_n^k$, c'est-à-dire pour les termes de la $k^{\text{ième}}$ colonne de P, défini à un facteur près de proportionnalité. Le tableau P lui-même n'est donc défini qu'à un produit près à droite par un tableau canonique. Pour résoudre complètement le problème proposé et passer de l'égalité (3) à la forme voulue pour $\mathbf{A}$, il suffit de montrer $\Delta(\mathrm{P}) \neq 0$. S'il n'en était pas ainsi, $\alpha_1, \alpha_2, \ldots, \alpha_n$ vérifieraient, quel que soit i, une même relation

$$u_1 \alpha_1 + u_2 \alpha_2 + \ldots + u_n \alpha_n = 0,$$

où nous pouvons supposer par exemple $u_n \neq 0$. Mais alors, en remplaçant dans chaque système (3 *bis*) la dernière égalité par la précédente relation, on en conclurait que les n nombres distincts $\lambda_1, \lambda_2, \ldots, \lambda_n$ vérifieraient la relation

$$\begin{vmatrix} a_1^1 - \lambda & a_1^2 & \ldots & a_1^{n-1} & a_1^n \\ \ldots\ldots & \ldots & \ldots & \ldots\ldots & \ldots \\ a_{n-1}^1 & a_{n-1}^2 & \ldots & a_{n-1}^{n-1} - \lambda & a_{n-1}^n \\ u_1 & u_2 & \ldots & u_{n-1} & u_n \end{vmatrix} = 0,$$

ce qui est absurde, cette relation étant de degré $n - 1$ en λ et non identiquement nulle. On peut donc énoncer le résultat :

Si l'équation en λ de $\mathbf{A}$ n'a pas de racine multiple, on peut mettre $\mathbf{A}$ sous la forme

$$\mathbf{A} = \mathrm{P}\,|\lambda_1, \lambda_2, \ldots, \lambda_n|\,\mathrm{P}^{-1},$$

$\lambda_1, \lambda_2, \ldots, \lambda_n$ sont les racines de l'équation en λ, et, leur ordre étant choisi, P est déterminé à un produit près à droite par un tableau canonique. Les rapports des termes de la $k^{\text{ième}}$ colonne sont des fonctions rationnelles de λ_k et des termes de $\mathbf{A}$. On verra

---

[1] Pour la discussion du cas général, je renvoie au *Traité* de M. Jordan ou à un Mémoire de H. Poincaré (*Journal de l'École Polytechnique*, 1881) ou encore à l'article de MM. Meyer et Drach sur les invariants (*Encyclopédie*, t. I, vol. II).

aisément ce que deviennent ces résultats pour la théorie des substitutions et le problème primitivement posé.

La condition du théorème n'est évidemment pas nécessaire et certains tableaux peuvent être mis sous la forme précédente sans que leur équation en λ ait des racines distinctes. Mais le début du raisonnement est toujours applicable, les nombres λ_k sont encore des racines de l'équation en λ, et les termes de la colonne correspondante de P sont donnés, avec plus ou moins d'indétermination, par un des systèmes (3 *bis*). Dans tous les cas on peut affirmer que : *λ_k s'exprime rationnellement en fonction des termes α_i^k de la $k^{\text{ième}}$ colonne de* P *et des termes de* A. Chaque fois qu'un tableau sera mis sous la forme précédente, nous dirons que $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ est son *tableau canonique* et P son *opérateur*. Le tableau canonique est toujours déterminé, l'opérateur est plus ou moins indéterminé (¹); il l'est même complètement si tous les λ sont égaux. On a, en effet, quel que soit P,

$$[\lambda] = \mathrm{P} \times [\lambda, \lambda, \ldots, \lambda] \times \mathrm{P}^{-1}.$$

Nous sommes maintenant en mesure de rechercher des ensembles abéliens. Il suffit de généraliser la propriété énoncée pour les tableaux canoniques : *si un ensemble abélien de tableaux renferme un tableau* A *dont l'équation en λ est à racines distinctes* (tableau canonique à termes distincts), *tous les autres tableaux de l'ensemble ont même opérateur que* A.

Soit, en effet, X un tableau de l'ensemble, on doit avoir

$$\mathrm{AX} = \mathrm{XA} \qquad \text{ou} \qquad \mathrm{A} = \mathrm{XAX}^{-1}.$$

Mais si A a pour tableau canonique E et pour opérateur P, on peut écrire l'égalité précédente

$$\mathrm{A} = \mathrm{XPEP}^{-1}\mathrm{X}^{-1} = (\mathrm{XP}) \times \mathrm{E} \times (\mathrm{XP})^{-1},$$

ce qui montre que XP est un opérateur de A, il ne peut différer

(¹) Cette indétermination peut encore se traduire par un produit près à droite par un tableau S, ce tableau étant le plus général avec lequel le tableau canonique E soit permutable. On peut, en effet, écrire alors :

$$\mathrm{PEP}^{-1} = \mathrm{PS} \times \mathrm{E} \times \mathrm{S}^{-1}\mathrm{P}^{-1} = \mathrm{PS} \times \mathrm{E} \times (\mathrm{PS})^{-1},$$

car

$$\mathrm{SES}^{-1} = \mathrm{ESS}^{-1} = \mathrm{E}.$$

de P que par le produit à droite par un tableau canonique E'. Donc

$$XP = PE \quad \text{ou} \quad X = PEP^{-1}.$$

Un tel ensemble peut notamment contenir tous les systèmes simples opérateur quelconque ; les opérations sur ses tableaux se réduisent à celles sur leurs tableaux canoniques. La condition imposée dans le théorème est peu restrictive, elle conduit à une catégorie assez générale d'ensembles abéliens, qui nous suffira par la suite.

Formes décomposables et équivalence.

Toutes les définitions et propriétés énoncées jusqu'ici s'appliquent indifféremment aux tableaux à termes quelconques. Nous aurons surtout à nous occuper des tableaux, tels qu'à toute colonne formée de termes imaginaires corresponde une colonne formée des termes imaginaires conjugués ; nous les appellerons *semi-réels*. Nous désignerons par r le nombre de colonnes réelles et par s le nombre de couples de colonnes imaginaires conjuguées ($r + 2s = n$, r ou s pouvant être nul).

On peut, en particulier, toujours mettre sous cette forme *l'opérateur d'un tableau à termes réels ;* les colonnes réelles correspondant aux racines réelles de l'équation en λ, les couples de colonnes imaginaires conjuguées aux couples de racines imaginaires conjuguées. Un tel opérateur P est encore défini, à un produit près, à droite par un tableau canonique E, mais E doit comprendre r termes réels et s couples de termes imaginaires conjugués, le rang de ces termes étant le même que celui des colonnes imaginaires de P. Pour abréger, nous dirons que le produit à droite d'un tableau P par un tableau canonique E qui lui correspond ainsi est une *dilatation*.

Les formes linéaires du système associé à un tableau semi-réel A se répartissent en r réels, $\xi_1, \xi_2, \ldots, \xi_r$ et s couples imaginaires conjugués, $\eta_1, \bar{\eta}_1, \eta_2, \bar{\eta}_2, \ldots, \eta_s, \bar{\eta}_s$. Leur produit

$$\Phi(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{i=n} (a_1^i x_1 + a_2^i x_2 + \ldots + a_n^i x_n)$$

est une forme homogène de degré n, *décomposable, à coefficients*

réels. Nous dirons encore que Φ est associée à A; mais réciproquement, si l'on se donne une telle forme Φ, les formes linéaires dont elle est le produit n'étant définies respectivement qu'à des facteurs près (réels pour les ξ_i, imaginaires conjugués pour les η_j, $\overline{\eta}_j$), *le tableau semi-réel, auquel Φ est associée, n'est défini qu'à une dilatation près de déterminant* 1.

On peut encore associer à A la fonction

$$F(x_1, x_2, \ldots, x_n) = f(\lambda_i |\xi_i|, \mu_j, \eta_j|),$$

f étant une fonction homogène de $r+s$ variables et λ_i, μ_j des paramètres positifs. L'un des avantages [1] d'une telle fonction, comme nous le verrons par la suite, est que le tableau auquel elle est associée n'est défini qu'à une dilatation près. C'est Hermite (*Journal de Crelle*, t. XLI) qui, le premier, utilisa une telle fonction; il prenait pour f une somme de carrés et F était par suite une *forme quadratique définie*

$$F(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{i=n} \lambda_i^2 |\xi_i|^2 + \sum_{j=1}^{j=s} \mu_j^2 \eta_j \overline{\eta_j}.$$

De même que pour le système de formes, la forme décomposable ou la fonction d'Hermite associée au tableau $A \times B$ se déduit par la substitution A de la forme ou de la fonction associée à B. Par suite, au point de vue de l'étude arithmétique des formes décomposables, il peut y avoir intérêt à considérer les substitutions Σ qui remplacent tout système de nombres entiers pour les x par un système de nombres entiers pour les ξ et réciproquement. Pour

---

[1] Pour plus de détails sur l'utilité de cette fonction, *voir* le Chapitre IV. A un autre point de vue, on pourrait encore associer à A la forme bilinéaire

$$\Sigma a_i^j x_i y_j,$$

qui devient une forme quadratique si, A étant symétrique, on fait $x_i = y_i$. Si A est symétrique gauche d'ordre pair, on peut lui associer de même un *complexe linéaire de droites*. Pour ces différents cas, il y aurait lieu de définir le tableau symétrique S_1 d'un tableau S (déduit par changement de lignes en colonnes). L'effet d'une substitution linéaire S est alors de remplacer A par SAS_1. Je renvoie pour ce sujet aux Traités sur les invariants, par exemple l'*Encyclopédie*, t. I, vol. II, article de Meyer et Drach.

cela, il faut et il suffit (¹) que Σ et Σ^{-1} soient à termes entiers, ou encore que Σ *soit à termes entiers et* $\Delta(\Sigma)$ *égal à* ± 1.

Un tel tableau est dit *unimodulaire*, et plus particulièrement modulaire si $\Delta(\Sigma) = +1$. D'après ce que nous venons de dire, l'inverse d'un tableau unimodulaire est encore unimodulaire; il en est encore de même du produit de plusieurs tableaux unimodulaires.

Deux tableaux A et B sont dits *équivalents* si A est le *produit à gauche de* B *par un tableau unimodulaire*

$$A = \Sigma B, \qquad \Delta(\Sigma) = \pm 1$$

(on dit proprement équivalent si Σ est modulaire); cette notion d'équivalence (²) est en somme transportée de la théorie des formes : suivant une locution déjà ancienne (elle remonte à Gauss, pour les formes binaires quadratiques) les formes décomposables associées à A et B sont dites *arithmétiquement équivalentes;* elles engendrent, à l'ordre près, les mêmes ensembles de valeurs quand on remplace les variables par tous les systèmes de n entiers. C'est Hermite qui, dans son célèbre Mémoire sur la transformation des fonctions abéliennes, étendit la notion aux tableaux et aux substitutions; nous en trouverons d'autres raisons d'être aux Chapitres suivants.

L'équivalence est réciproque, $A = \Sigma B$ entraîne en effet $B = \Sigma^{-1} A$ et Σ^{-1} est également unimodulaire. En outre, deux tableaux équivalents à un troisième sont équivalents entre eux; car

$$\begin{matrix} B = \Sigma A \\ C = \Sigma' A \end{matrix} \qquad \text{entraîne} \qquad B = \Sigma \Sigma'^{-1} C.$$

(¹) Il suffit évidemment que Σ et Σ^{-1} soient à termes entiers, on constate que cela est nécessaire en considérant les systèmes d'entiers

$$(1, 0, \ldots, 0), \quad (0, 1, 0, \ldots, 0), \quad \ldots.$$

D'autre part $\Delta(\Sigma)$ et $\frac{1}{\Delta(\Sigma)}$ devant être entiers, il faut $\Delta(\Sigma) = \pm 1$, mais alors, d'après la formation des termes de Σ^{-1}, on voit qu'ils sont entiers si ceux de Σ le sont.

(²) Pour la notion d'équivalence, il y a la même ambiguïté que pour la définition du produit et l'association d'un système de formes à un tableau. Dans le Mémoire d'Hermite, la multiplication par Σ est à droite; pour d'autres points de vue (formes bilinéaires, recherches de M. Jordan), on peut envisager le produit par des tableaux unimodulaires, simultanément à droite et à gauche $\Sigma A \Sigma'$.

L'ensemble des tableaux équivalents à un tableau donné, est dit, toujours suivant une locution de la théorie des formes, un *système* de tableaux, deux éléments de ce système sont équivalents; ou, encore, il peut être engendré à partir de l'un quelconque de ses éléments. On dit que ce système est une classe, si l'on se borne à l'équivalence propre.

Langage géométrique.

Pour simplifier, ou pour illustrer certains énoncés ou démonstrations, il peut être commode d'employer un langage géométrique. On dit alors qu'un système de n nombres réels $p_1, p_2, \ldots, p_n$ représente un *point* P *de l'espace à n dimensions* ([1]); les nombres sont les *coordonnées du point*. Nous étendrons aussi ce langage, au cas où parmi les nombres p_i, r seulement sont réels, et $2s$ imaginaires conjugués deux à deux. A l'instar des tableaux, nous dirons que l'*espace* est alors semi-réel.

Nous pourrions interpréter une substitution linéaire, soit comme une correspondance entre points d'un même espace, soit, et c'est toujours à ce dernier point de vue que nous nous placerons, comme un changement de coordonnées, sans changement d'origine. D'une façon précise, étant donné un point $\mathrm{P}(p_1, p_2, \ldots, p_n)$ et un tableau T, nous appellerons *coordonnées relatives de* P *par rapport à* T, les nombres $x_1, x_2, \ldots, x_n$ définis par

$$\| p_1 \quad p_2 \quad \ldots \quad p_n \| = \| x_1 \quad x_2 \quad \ldots \quad x_n \| \cdot \mathrm{T};$$

les nombres p, auxquels nous attacherons plus d'importance, seront dits, par opposition, *coordonnées absolues*. On peut faire à ce sujet plusieurs remarques : d'abord l'origine, c'est-à-dire le point $(0, 0, \ldots, 0)$, conserve les mêmes coordonnées; ensuite les lignes de T sont formées par les coordonnées absolues des points dont les coordonnées relatives sont respectivement

$$(1, 0, \ldots, 0), \quad (0, 1, 0, \ldots, 0), \quad \ldots, \quad (0, 0, \ldots, 1).$$

([1]) Ce langage est très courant en analyse et théorie des ensembles et des fonctions. Pour les mêmes raisons que pour les tableaux, il m'a paru utile de fixer ici les notations employées dans la suite de ces leçons. Je signale qu'on peut envisager aussi $p_1, p_2, \ldots, p_n$ comme les coordonnées homogènes d'un point d'un espace à $n-1$ dimensions ou encore comme les projections d'un *vecteur libre*.

En se plaçant, par exemple, dans le cas de trois dimensions et en supposant l'espace réel ainsi que les termes de T, ces points sont sur les nouveaux axes de coordonnées. Pour avoir un véritable changement de coordonnées, au sens habituel du mot, il faudrait qu'ils fussent à distance 1 de l'origine. S'il n'en est pas ainsi, on peut considérer que le changement de coordonnées a été combiné avec le choix d'une unité de longueur particulière sur chaque axe. Enfin une dernière remarque essentielle : si l'espace est semi-réel, en prenant pour T un tableau de r colonnes réelles et $2s$ imaginaires conjuguées, rangées dans le même ordre que les coordonnées absolues, chaque point aura par rapport à T des *coordonnées relatives réelles*. On pourra, en particulier, choisir T de façon que ces coordonnées relatives soient formées des coordonnées réelles et des parties réelles et imaginaires des autres. Ainsi

$$(p_1 \quad p_2 + ip'_2 \quad p_2 - ip'_2) = (p_1 \quad p_2 \quad p'_2) \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & i & -i \end{Vmatrix}.$$

En adoptant une définition de la théorie des vecteurs, nous appellerons *somme* et *différence* de deux points $(p_1, \ldots, p_n)$, $(q_1, \ldots, q_n)$ les points $(p_1 + q_1, \ldots, p_n + q_n)$, $(p_1 - q_1, \ldots, p_n - q_n)$. C'est une notion invariante pour les changements de coordonnées envisagés; on voit, pour cette invariance, la nécessité de ne point changer d'origine.

Enfin, en étendant la notion d'équation de plan et d'équations de droite de l'espace à trois dimensions, nous appellerons *sous-espace linéaire de dimension m*, $(m < n)$ l'ensemble des points vérifiant les $n - m$ équations

$$u_i^1 p_1 + u_i^2 p_2 + \ldots + u_i^n p_n = v_i \qquad (i = 1, 2, \ldots, n - m);$$

les premiers membres sont des formes linéaires indépendantes, en outre les coefficients des coordonnées imaginaires conjuguées sont aussi imaginaires conjugués; nous continuerons d'appeler *droite* (1) un sous-espace de dimension 1. La définition des sous-espaces est indépendante des coordonnées choisies, absolues ou relatives; en

(1) M. Minkowski appelle également *plan* un sous-espace linéaire de dimension $n - 1$.

passant d'un système à l'autre, les coefficients des équations se transforment par une substitution liée ([1]) simplement à T. La solution générale des équations dépend de m paramètres arbitraires et s'exprime au moyen d'une solution particulière quelconque $(\varpi_1, \varpi_2, \ldots, \varpi_n)$ et de m solutions des équations sans deuxièmes membres quelconques, mais *indépendantes*, c'est-à-dire telles que la matrice qu'elles forment

$$M = \begin{Vmatrix} \alpha_1^1 & \alpha_1^2 & \ldots & \alpha_1^n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_m^1 & \alpha_m^2 & \ldots & \alpha_m^n \end{Vmatrix},$$

de type (m, n), soit de rang m. Les solutions sont alors

$$\| p_1 \quad p_2 \quad \ldots \quad p_n \| = \| \varpi_1 \quad \varpi_2 \quad \ldots \quad \varpi_n \| + \| r_1 \quad r_2 \quad \ldots \quad r_m \| \times M.$$

Les nombres r sont des indéterminées réelles ([2]), en outre chaque solution n'est ainsi exprimée qu'une fois, de sorte que l'on peut appeler les r, *coordonnées du point dans le sous-espace, relatives à l'origine* $(\varpi_1, \varpi_2, \ldots, \varpi_n)$ *et à la matrice* M; les r sont réciproquement des fonctions linéaires et homogènes de m différences $p_i - \varpi_i$ convenablement choisies (correspondant à un mineur non nul de M).

Dans le cas où le sous-espace passe par l'origine, on peut supposer

$$\varpi_1 = \varpi_2 = \ldots = \varpi_n = 0$$

et M que nous appellerons *matrice du sous-espace* ([3]) est formé par m points du sous-espace. On peut traduire le fait que M est de rang m en disant que les m points n'appartiennent pas à un sous-espace de rang inférieur (s'il en était ainsi, ils vérifieraient en effet plus de $n - m$ relations et le rang de leur matrice serait inférieur

---

([1]) C'est la substitution associée à $(T_1)^{-1}$ (*voir* une précédente Note); on la désigne, dans la théorie des invariants, sous le nom de *substitution contravariante* de T.

([2]) Cette condition de réalité résulte de ce que l'espace est semi-réel; aux colonnes réelles de la matrice doivent correspondre des p réels, aux colonnes imaginaires conjuguées des p imaginaires conjugués. En rapprochant ceci d'une remarque précédente, on voit que la notion d'espace semi-réel n'est en somme qu'une représentation non entièrement réelle d'un espace réel.

([3]) Dans le cas général, M serait, en quelque sorte, formé par m directions indépendantes du sous-espace.

à m. La donnée des équations peut être remplacée par celle d'un tel système de m points; il y a en outre une assez grande latitude dans ce choix, et l'on peut, en particulier, choisir ces m points dans un ensemble donné *a priori* dont les points appartiennent au sous-espace, mais n'appartiennent pas à un sous-espace de dimension moindre. On choisira pour cela un premier point A_1 de l'ensemble, différent de O; ensuite un deuxième point de l'ensemble A_2 non situé dans le sous-espace à une dimension défini par O et A_1; ensuite un point A_3, non situé dans le sous-espace à deux dimensions défini par O, A_1, A_2; .... Pour passer d'un tel système de m points à un système de $n-m$ équations, qui sont alors homogènes, il suffit de prendre pour coefficients de ces équations $n-m$ solutions indépendantes du système

$$a^i_1 y_1 + a^i_2 y_2 + \ldots + a^i_n y_n = 0 \qquad (i = 1, 2, \ldots, m),$$

$a^i_1, \ldots, a^i_n$ étant les coordonnées de A_i.

Considérons encore le cas d'une *droite* quelconque. Il suffit alors de se donner deux points *distincts* $A(a_1, a_2, \ldots, a_n)$ et $B(b_1, b_2, \ldots, b_n)$ (coordonnées absolues ou relatives); un point quelconque M de la droite a alors pour coordonnées (absolues ou relatives)

$$x_1 = \frac{\alpha_1 + t\beta_1}{1+t}, \qquad x_2 = \frac{\alpha_2 + t\beta_2}{1+t}, \qquad \ldots, \qquad x_n = \frac{\alpha_n + t\beta_n}{1+t},$$

t étant une variable *réelle*. On voit que, t variant continûment de 0 à ∞, le point M *se déplace* de A à B, sans aller à l'infini. Pour cette raison, nous dirons que les points correspondants à ces valeurs de t forment le *segment* (¹) AB.

Distance généralisée.

En étendant à l'espace réel à n dimensions des résultats obtenus géométriquement pour l'espace à trois, on peut encore appeler *distance de deux points* l'expression

$$[(\alpha_1 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 + \ldots + (\alpha_n - \beta_n)^2]^{\frac{1}{2}},$$

(¹) M. Minkowski étend cette définition au cas des sous-espaces quelconques, on obtient alors ce qu'il appelle des *cellules*.

ou plus généralement, en ne supposant pas les axes rectangulaires

$$[F(\alpha_i - \beta_i)]^{\frac{1}{2}},$$

F étant une forme quadratique *définie positive*. Mais il n'est pas toujours nécessaire d'employer cette fonction précise et notamment pour les questions de voisinage, on peut utiliser une fonction des différences des coordonnées simplement assujettie à devenir infiniment petite en même temps que ces différences. Pour se rapprocher plus de la notion de distance géométrique, on peut en outre s'imposer que cette fonction soit indépendante de l'ordre des points, s'additionne pour des segments placés bout à bout sur une même droite et enfin conserve la droite comme plus court chemin.

On est ainsi conduit aux conditions énoncées (¹) par M. Minkowski dans sa *Geometrie der Zahlen* et que je cite, d'après lui, avec quelques restrictions afin de comprendre le cas d'un espace semi-réel : on appelle *distance généralisée* de deux points A, B, une fonction des différences des coordonnées des points

$$S(AB) = f(\alpha_i - \beta_i),$$

cette fonction étant *réelle, définie pour deux points quelconques de l'espace considéré* et telle que

$$\begin{cases} (1) & \begin{cases} f(u_i) \geq 0, \\ f = 0 \quad \text{entraînant} \quad u_i = 0, \end{cases} \\ (2) & f(\lambda u_i) = |\lambda| f(u_i) \qquad (\lambda \text{ réel}), \\ (3) & f(u_i + v_i) \leq f(u_i) + f(v_i). \end{cases}$$

La condition (2) entraîne immédiatement l'égalité (²)

$$S(AB) + S(BC) = S(AC)$$
$$(B \text{ sur le segment } AC);$$

(¹) Les définitions et énoncés de la fin de ce Chapitre sont empruntées, bien entendu, à la *Geometrie der Zahlen* ou aux *Diophantische Approximationen*.

(²) Je ne me suis pas cru tenu de traduire rigoureusement l'expression de M. Minkowski : *Strähldistanz*. De même, les conditions données par lui sont moins restrictives en général ; il distingue notamment la *Strähldistanz*, les *Strähldistanz einhellig*, *wechselseitig*, ou les deux, suivant qu'elle vérifie les propriétés (1 — 2 pour $\lambda > 0$) ; (1 — 2 pour $\lambda > 0$ — 3) ; (1 — 2) ; (1 — 2 — 3).

en effet les coordonnées de A, C, B étant respectivement

$$\alpha_i, \quad \gamma_i, \quad \frac{\gamma_i - \lambda\alpha_i}{1-\lambda}, \qquad \lambda \geqq 0,$$

on a, d'après (2) appliquée au cas $\lambda \geqq 0$,

$$S(AB) = f\left(\frac{\gamma_i - \lambda\alpha_i}{1-\lambda} - \alpha_i\right) = \frac{1}{1-\lambda} f(\gamma_i - \alpha_i),$$

$$S(BC) = f\left(\gamma_i - \frac{\gamma_i - \lambda\alpha_i}{1-\lambda}\right) = \frac{\lambda}{1-\lambda} f(\gamma_i - \alpha_i),$$

$$S(AB) - S(BC) = f(\gamma_i - \alpha_i) = S(AC);$$

la même condition (2), où l'on fait $\lambda = -1$, entraîne

$$S(AB) = S(BA).$$

Enfin la condition (3) peut s'écrire

$$(3') \qquad S(AB) + S(BC) \geqq S(AC);$$

sous cette forme, c'est l'inégalité connue entre les trois côtés d'un triangle qui entraîne la propriété du plus court chemin.

Si l'on fait un changement de coordonnées, la fonction f devient une fonction φ des différences ξ_i des coordonnées relatives; les u étant des fonctions linéaires et homogènes des ξ, φ vérifie les mêmes conditions que f; cette remarque permet de supposer, dans les applications de la distance généralisée, sinon l'espace réel, au moins les coordonnées de chaque point toutes réelles.

Appliquons notamment ceci à la continuité de f. On a, en supposant les u réels, la suite d'inégalités

$$f(u_1, u_2, \ldots, u_n) \leqq f(u_1, 0, \ldots, 0) + f(0, u_2, \ldots, 0) + \ldots + f(0, 0, \ldots, u_n)$$
$$\leqq (|u_1| + |u_2| + \ldots + |u_n|)K,$$

K étant un nombre supérieur à tous les nombres $f(1, 0, \ldots, 0)$, $f(0, 1, \ldots, 0)$, ..., $f(0, 0, \ldots, 1)$. Ceci montre bien qu'on peut obtenir [1] une limitation supérieure donnée de f en limitant convenablement les $|u|$. Si les u n'étaient que des coordonnées relatives, leur limitation supérieure pourrait être obtenue en limitant convenablement les coordonnées absolues. La réciproque est également

[1] On compare en somme la distance généralisée de A à B à la somme des distances des segments du *contour des coordonnées* de A à B.

exacte, on peut obtenir une limitation supérieure donnée des $|u|$ par une limitation convenable de f. En effet, considérons les valeurs de u telles que $|u_1|^2 + |u_2|^2 + \ldots + |u_n|^2 = 1$, ces valeurs sont des fonctions continues de $n - 1$ variables; f est une fonction continue, définie et positive des mêmes variables, elle a un minimum g qu'elle atteint et qui, par conséquent, n'est pas nul. Mais alors il suffit de prendre f inférieur à $g\varepsilon$ pour pouvoir affirmer que les $|u|$ ne dépassent pas ε. Car s'il n'en était pas ainsi, le nombre ρ tel que

$$|u_1|^2 + |u_2|^2 + \ldots + |u_n|^2 = \rho^2$$

serait supérieur ou égal à ε; mais d'après ce qui a été dit, $f\left(\frac{u_i}{\rho}\right)$ devrait être au moins égal à g, donc $f(u_i)$ au moins égal à ρg et *a fortiori* à εg, ce qui est absurde. On peut encore traduire ces deux propriétés en disant que : *Étant données deux distances généralisées, toute limite supérieure pour l'une entraîne une limite supérieure pour l'autre, et réciproquement.*

Exemples de distances. — Nous avons obtenu les conditions (5) en traduisant algébriquement certaines propriétés de la distance géométrique. L'expression analytique de cette distance vérifie évidemment ces conditions (5); il en est de même de son extension immédiate à l'espace semi-réel général

$$f(u_i) = (|u_1|^2 + |u_2|^2 + \ldots)^{\frac{1}{2}},$$

la somme étant seulement étendue aux valeurs absolues des coordonnées. Les deux premières propriétés sont immédiates, on vérifiera la troisième en élevant au carré les deux membres de l'inégalité et effectuant les réductions. On a un autre exemple de distance en prenant S(AB) égal au maximum des valeurs absolues des différences de coordonnées

$$f(u_i) = \text{maximum de } (|u_1|, |u_2|, \ldots);$$

ici encore la vérification est immédiate et résulte de la propriété bien connue de la valeur absolue d'une somme. Cette distance est appelée *spanne* (¹) par Minkowski et *distance réduite* par

(¹) La traduction littérale du mot allemand serait *empan* ou longueur de la main ouverte du pouce à l'index.

J. Tannery. Citons encore l'*écart* [1] de M. Jordan, somme des valeurs absolues des différences des coordonnées

$$f(u_i) = \Sigma |u_i|.$$

En partant de ces exemples, on peut obtenir d'autres distances généralisées. Remarquons que, pour chacun d'eux, la distance est seulement fonction des valeurs absolues des différences des coordonnées

$$f(u_i) = \varphi(|\xi_i|, |\eta_j|),$$

$\xi_1, \xi_2, \ldots, \xi_r$ étant les différences réelles et $\eta_1, \overline{\eta}_1, \ldots, \eta_s, \overline{\eta}_s$ les s couples de différences imaginaires conjuguées. D'une part, remplaçons $|\xi_i|$ et $|\eta_j|$ par $\lambda_i|\xi_i|$, $\mu_j|\eta_j|$, les λ et les μ étant $r+s$ constantes positives données. D'autre part, faisons un changement de coordonnées

$$\| u_1 \ \ldots \ u_n \| = \| x_1 \ \ldots \ x_n \| \, \mathrm{A}, \qquad \Delta(\mathrm{A}) \neq 0,$$

A étant choisi de façon que les x soient réels. En considérant dans φ les ξ et les η comme des formes linéaires des x, on obtient ainsi une fonction de n variables réelles

$$(6) \qquad \begin{aligned} \mathrm{F}(x_1, x_2, \ldots, x_n) &= \varphi(\lambda_i|\xi_i|, \mu_j|\eta_j|) \\ &= \varphi(|\lambda_i\xi_i|, |\mu_j\eta_j|) \end{aligned}$$

qui vérifie encore les conditions imposées. Elle est réelle, positive et définie pour tout système de valeurs des x, car à ce système correspond dans f des valeurs des u,

$$\lambda_1\xi_1, \ \ldots, \ \lambda_r\xi_r, \quad \mu_1\eta_1, \ \mu_1\overline{\eta_1}, \ \ldots, \ \mu_s\eta_s, \ \mu_s\overline{\eta_s},$$

qui appartiennent bien à l'espace considéré. D'autre part, f ne peut s'annuler que si toutes les valeurs précédentes et, par suite, les x sont nuls [puisque $\Delta(\mathrm{A}) \neq 0$] ; l'homogénéité et le degré se conservent évidemment. Enfin, si l'on remplace x_i par $x_i + x'_i$, on

---

(²) Ces deux exemples pourraient être considérés comme des cas particuliers de

$$f(u_i) = [\Sigma |u_i|^\omega]^{\frac{1}{\omega}},$$

le premier pour ω infini, le deuxième pour $\omega = 1$. L'expression générale est aussi une distance généralisée pour $\omega > 1$, mais la vérification en est plus malaisée.

remplace par ce fait $\lambda_i \xi_i$ par $\lambda_i(\xi_i + \xi'_i)$ et $\mu_j \eta_j$, $\mu_j \bar{\eta}_j$ par $\mu_j(\eta_j + \eta'_j)$, $\mu_j(\bar{\eta}_j + \bar{\eta}'_j)$ et, par conséquent, dans f, u_i par $u_i + u'_i$; la troisième condition est aussi vérifiée. Nous avons déjà signalé l'avantage qu'il pouvait y avoir à associer à un tableau une fonction de la forme (6), nous verrons plus tard pourquoi lui imposer les conditions (5). Pour le premier exemple, cette fonction devient la racine carrée de la forme quadratique d'Hermite

$$(6\ bis) \qquad F(x_1, x_2, \ldots, x_n) = \left[\Sigma \lambda_i^2 \xi_i^2 + \Sigma \mu_j^2 \eta_j \bar{\eta}_j\right]^{\frac{1}{2}};$$

nous utiliserons, de préférence, le deuxième exemple que nous appellerons la *spanne à r + s paramètres*, ou plus simplement la spanne, quand il n'y aura pas ambiguïté

$$(6\ ter) \qquad F(x_1, x_2, \ldots, x_n) = \text{maximum}(\lambda_i |\xi_i|, \mu_j |\eta_j|).$$

Corps caractéristique. — En se plaçant pour fixer les idées dans l'espace réel à trois dimensions, la distance généralisée est, pour des segments parallèles entre eux, proportionnelle à leur longueur. L'adoption de cette distance revient donc à choisir pour chaque *direction* de droite, une unité de longueur particulière ([1]); de sorte que, pour caractériser une distance déterminée, on peut mener, par l'origine, des segments OM égaux à l'unité de longueur pour leur direction. Le lieu de ces segments forme un *corps* ou *volume* et le lieu des points M, qui sont à une distance 1 de O, la *surface frontière* de ce corps; nous les appellerons, suivant M. Minkowski, *corps et surface caractéristique de la distance envisagée*. Leur définition s'étend sans difficulté à l'espace à n dimensions même semi-réel, ce sont respectivement les ensembles de points M tels que

$$S(OM) \leqq 1 \qquad \text{et} \qquad S(OM) = 1.$$

D'après les propriétés de continuité de S, le premier de ces ensembles est *un domaine*, en ce sens que si un point A en fait partie, égalité exclue, tout point infiniment voisin de A (différences des coordonnées inférieures, en valeur absolue, à ε suffisamment petit) est encore intérieur au sens étroit; ceci en raison de la

---

([1]) On pourrait comparer ceci aux corps cristallisés où les propriétés sont variables avec les directions.

continuité de la distance généralisée ; en outre, *il est borné*, une limitation de S(OM) entraînant une limitation de la spanne. La surface caractéristique est *la frontière du corps* [1], car c'est l'ensemble des points limites à la fois pour l'ensemble et pour l'ensemble complémentaire.

Pour trouver ces premiers résultats, nous n'avons utilisé que la première propriété (1) et la continuité de f. On peut aussi traduire en propriétés géométriques du corps caractéristique les deux dernières conditions. La deuxième condition pour $\lambda = -1$ peut s'énoncer en disant que le corps et la surface sont *symétriques par rapport à l'origine*, c'est-à-dire renferment à la fois $(x_1, x_2, \ldots, x_n)$ et $(-x_1, -x_2, \ldots, -x_n)$. Enfin les conditions (2) pour $\lambda > 0$ et (3) entraînent ce fait que si deux points A, B sont dans le corps, tout point du segment AB est dans le corps et même, au sens étroit, si l'un des points est intérieur au sens étroit [2]. C'est ce qui résulte de l'inégalité (pour $t > 0$)

$$f\left(\frac{x_i + t\xi_i}{1+t}\right) \leq \frac{1}{1+t} f(x_i) + \frac{t}{1+t} f(\xi_i).$$

M. Minkowski exprime ce fait en disant que le corps est *nulle part concave* (il réserve le mot *convexe* pour le cas plus spécial où aucun segment de droite n'est situé sur la surface). Le segment AB étant un cas particulier d'un chemin continu, le corps est d'un seul tenant et simplement connexe. Comme exemples de corps caractéristiques dans l'espace à trois dimensions, citons : la *sphère* pour la distance ordinaire, le *parallélipipède* pour la spanne $(|x|, |y|, |z|) \leq 1$ et l'*octaèdre* pour l'écart. En supposant que cet espace provient par changement de coordonnées de l'espace semi-réel $(x, y + iz, y - iz)$, on trouve pour corps caractéristiques : encore la *sphère*, un *cylindre circulaire* ou *elliptique* limité à deux bases, $(|x|, \sqrt{y^2 + z^2}) \leq 1$, et *deux cônes* ayant leurs sommets sur ox et une même base dans le plan des y, z.

---

(1) *Voir* sur ces notions et d'autres analogues de la théorie des ensembles, par exemple le *Cours d'Analyse* de M. Jordan.

(2) Cette propriété est susceptible d'une réciproque facile à établir et qu'il ne m'a pas paru utile de développer ici.

Enfin, le corps caractéristique peut être défini, ainsi que dans l'espace à trois dimensions, comme un lieu de segments. En considérant par exemple tous les points A dont la vraie distance à O est 1 et pour chacun de ces points le point B,

$$\mathrm{B} = \rho\mathrm{A}, \qquad \frac{1}{\rho} = S(\mathrm{OA});$$

le point B est sur la surface caractéristique et le segment OB intérieur au corps. Réciproquement, on constate, sans peine, que tout point intérieur au corps appartient à un tel segment et à un seul. Cette remarque conduit à l'existence du *volume* du corps caractéristique. On appelle ainsi (*voir* Jordan) *l'intégrale,* si elle existe, $\int \cdots \int dx_1, \ldots, dx_n$, *étendue à l'ensemble des points du corps.* Dans le cas où certains des x seraient imaginaires, on ramène au cas réel par un changement de variables fait en appliquant la règle habituelle. Ceci fait, un nouveau changement de variables ramène à l'intégrale $n - 1$-*uple* $\int \frac{1}{n} \rho\, d\sigma$ dont l'existence est manifeste, ρ étant continu; $d\sigma$ représente l'élément d'*aire* de la sphère

$$x_1^2 + \ldots + x_n^2 = 1.$$

Nous avons défini le corps caractéristique à partir de l'origine et du nombre 1; on peut de même définir un corps $\Gamma_k(\mathrm{A})$ à partir d'un point quelconque A, $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, et d'une constante positive k. Nous appellerons ainsi l'ensemble des points m tels que

$$S(\mathrm{AM}) \leq k.$$

On le déduit du corps caractéristique par une translation et une homothétie, c'est-à-dire que si $(x_1, x_2, \ldots, x_n)$ est un point quelconque du corps caractéristique, tous les points du nouveau corps sont donnés par

$$\alpha_1 + kx_1, \qquad \alpha_2 + kx_2, \qquad \ldots, \qquad \alpha_n + kx_n.$$

Si J est le volume du corps caractéristique $\Gamma_1(\mathrm{o})$, le volume de $\Gamma_k(\mathrm{A})$ est (en faisant dans l'intégrale le changement de variables) k^nJ.

Si l'on envisage un nombre fini de corps Γ, ils forment un domaine

(non nécessairement d'un seul tenant) *encore mesurable* et dont le volume est égal à la somme des volumes, si les corps n'ont pas de points communs, et lui est au plus égal dans le cas contraire. Avant de quitter cette question des volumes, remarquons que, même dans le cas de l'espace semi-réel, si un domaine est contenu dans un autre (au sens ordinaire), son volume lui est au plus égal, ceci parce que chaque élément des intégrales est essentiellement positif.

CHAPITRE II.

THÉORIE DES MODULES DE POINTS.

Dans la définition générale d'un *groupe* on envisage des éléments assujettis à un mode de composition associative (et commutative pour les groupes abéliens). On pourrait donc appliquer cette définition à des ensembles de nombres, en prenant comme mode de composition l'addition. On réserve habituellement le mot *groupe de nombres* pour le cas où ce mode de composition est la multiplication et, suivant une locution de M. Dedekind, on désigne par *module* un ensemble de nombres qui comprend la somme et la différence de deux quelconques d'entre eux. L'origine de cette dénomination est que l'ensemble des multiples d'un entier, ou même d'un nombre quelconque a, qui sont appelés par Gauss *congrus, module* a, forment un module au sens précédemment indiqué. Il est commode, ainsi qu'on le verra par la suite, de transporter cette notion de module aux points d'un espace à n dimensions, c'est-à-dire à des systèmes de n nombres. On suit en cela l'exemple de M. Minkowski, qui a utilisé les systèmes de points ayant pour coordonnées des nombres entiers (*Zahlengitter* ou *grille de nombres*) et de H. Poincaré qui a étudié l'arithmétique des réseaux de points dans le plan (*Journ. Éc. Polyt.*, 1880).

Dimension d'un module.

Nous appellerons donc *module de points*, dans un espace de dimension n réel ou semi-réel, un ensemble de points tel que la somme et la différence de deux d'entre eux appartiennent encore à l'ensemble. Un module comprend donc nécessairement l'origine (point à coordonnées toutes nulles), suivant une remarque déjà faite, sa définition est indépendante du système de coordonnées, absolues ou relatives.

La notion d'*isomorphisme*, qu'on définit pour des groupes abstraits quelconques, s'étend par conséquent aux modules; rappelons la définition appliquée à ce cas particulier : un module de points $\mathcal{A}$ est dit *isomorphe à un module de points* $\mathcal{B}$, si l'on peut établir entre leurs éléments une correspondance telle que [1] :

1° A tout point de $\mathcal{B}$ corresponde *un et un seul* point de $\mathcal{A}$;

2° A tout point de $\mathcal{A}$ corresponde *au moins* un point de $\mathcal{B}$;

3° A la somme et à la différence de deux points de $\mathcal{B}$ correspondent la somme et la différence des points correspondants de $\mathcal{A}$.

L'isomorphisme est dit *holoédrique* s'il est réciproque, c'est-à-dire si $\mathcal{B}$ est aussi isomorphe à $\mathcal{A}$, ou encore si, à tout point de $\mathcal{A}$, ne correspond qu'un point de $\mathcal{B}$; deux modules, isomorphes holoédriquement à un troisième, le sont aussi entre eux. Si l'isomorphisme n'est pas réciproque, on le dit *mériédrique*. Mais, même dans le premier cas, il n'y a pas toujours lieu de remplacer l'étude d'un module par celle d'un module isomorphe. Cette correspondance peut n'être due qu'à un changement de notations (par exemple un changement de coordonnées), et alors les figures géométriques sont les mêmes, à des déplacements ou des transformations simples près. Cependant, de même qu'il y a intérêt à considérer un système de deux figures égales, il peut y avoir intérêt à différencier des modules isomorphes considérés simultanément; par exemple, les multiples de 2 ou de 4 sont des modules isomorphes, mais, considérés simultanément, ils ont des propriétés différentes. Il peut se faire aussi que la différence soit plus profonde, les aspects géométriques étant dissemblables et l'isomorphisme ne traduisant qu'une ressemblance de constitution. Quelques exemples simples vont nous permettre d'illustrer ces divers cas et de prévoir les distinctions qu'il y aura à faire par la suite.

Imaginons d'abord, sur une droite, une suite de points illimitée dans les deux sens

$$\ldots,\quad A_{-2},\quad A_{-1},\quad O,\quad A_1,\quad A_2,\quad \ldots$$

la distance de deux points consécutifs étant constante. Prenons

---

[1] Les deux modules n'ont pas le même rôle dans cette définition. L'étymologie d'isomorphe justifie l'ordre adopté : $\mathcal{A}$ a une constitution analogue à celle de $\mathcal{B}$, mais $\mathcal{B}$ peut être plus complexe que $\mathcal{A}$.

l'un d'eux, O, comme origine, les coordonnées des points sont de la forme $k\alpha$, k étant un entier quelconque. Nous avons là un exemple de module de points dans un espace à une dimension; c'est même l'exemple le plus simple, à part celui formé par la seule origine; car, si un module comprend O et A_1, il comprend nécessairement A_2, tel que $\overline{A_1A_2} = \overline{OA_1}$, ... Imaginons cette même droite et ces mêmes points dans un plan rapporté à deux axes de coordonnées Ox, Oy, distincts de la droite; les coordonnées des points A sont de la forme $(k\alpha, k\beta)$. Nous avons, cette fois, un module dans un espace à deux dimensions, il est isomorphe holoédriquement au précédent, mais n'en est pas non plus distinct au point de vue géométrique.

Considérons encore dans un plan un quadrillage illimité, ou un réseau de parallélogrammes, et rapportons les points de ce quadrillage à l'un d'eux, O, comme origine, et à deux axes Ox, Oy. Les coordonnées sont de la forme $(u\alpha + v\alpha', u\beta + v\beta')$, u et v étant des entiers quelconques; les points recouvrent cette fois tout le plan [1]. Projetons-les sur une droite passant par l'origine, les projections ont, pour abscisses sur la droite, $(up + vq)$, elles forment un module isomorphe au précédent, même holoédriquement, si, sur toute parallèle à la direction des projetantes, il n'y a au plus qu'un seul point du quadrillage (il suffit pour cela que cette direction ait, par rapport à deux droites du quadrillage, un coefficient angulaire irrationnel). Mais, cette fois, la contexture géométrique des deux modules est très différente : tandis que, pour le premier, on peut fixer une limite inférieure à la distance de deux points, il n'en est plus de même du second, ainsi que nous le verrons, d'une façon précise, par la suite. On voit immédiatement comment l'exemple précédent s'étend à l'espace à trois dimensions (réseau de parallélipipèdes) et même à l'espace à n. En projetant ces modules sur des espaces de dimension moindre, on obtient toute une première catégorie de modules que nous appellerons *finis*, les seuls que nous étudierons en détail.

En se reportant aux deux premiers exemples, on est conduit à une première distinction entre les modules de points $\mathcal{M}$ d'un

---

(1) Cette figure géométrique est identique aux réseaux de Bravais (*voir* H. Poincaré, *loc. cit.*).

espace de dimension n, réel ou semi-réel, suivant que les points de $\mathcal{A}$ couvrent tout l'espace, ou, au contraire, appartiennent tous à un sous-espace linéaire contenant naturellement l'origine. Nous appellerons *dimension m du module* $\mathcal{A}$ la dimension du sous-espace de plus petite dimension qui contient tous les points de $\mathcal{A}$ (les coordonnées de ces points vérifient m relations indépendantes). On peut considérer un tel module comme identique géométriquement à un module $\mathcal{B}$ d'un espace à m dimensions.

D'une façon précise, $\mathcal{A}$ *est isomorphe holoédriquement à un module* $\mathcal{B}$ *de dimension m dans un espace à m dimensions;* il suffit de prendre pour $\mathcal{B}$ l'ensemble des points ayant pour coordonnées les coordonnées relatives des points de $\mathcal{A}$ par rapport à une matrice quelconque M de type (m, n) et de rang m, du sous-espace qui le contient; c'est-à-dire $(r_1, r_2, \ldots, r_m)$, tels que

$$(1) \qquad \| p_1 \quad p_2 \quad \ldots \quad p_n \| = \| r_1 \quad r_2 \quad \ldots \quad r_m \| \times \mathrm{M}.$$

Ce module $\mathcal{B}$ est, d'après sa constitution même, isomorphe à $\mathcal{A}$ (les relations entre les p et les r étant linéaires, la somme se conserve); l'isomorphisme est holoédrique, car un système de r ne peut évidemment provenir que d'un système de p. Enfin, $\mathcal{B}$ est de dimension $n - m$, sinon les r et, par suite, les p s'exprimeraient en fonction de moins de $n - m$ indéterminées, et il y aurait entre les coordonnées des points de $\mathcal{A}$ plus de m relations indépendantes.

Nous pouvons supposer que les lignes de la matrice M, qui sert à définir $\mathcal{B}$, sont les coordonnées de points de $\mathcal{A}$, d'après un raisonnement fait au premier Chapitre, pour un ensemble quelconque de points. Si, réciproquement, il existe une matrice de rang m formée avec m points d'un module $\mathcal{A}$ et pas de matrice de rang supérieur, $\mathcal{A}$ est de dimension m. Nous dirons que toute matrice ainsi formée est une *matrice du module;* elle devient un *tableau du module* (à déterminant non nul), si la dimension de $\mathcal{A}$ est égale à celle de l'espace.

Modules types.

Examinons d'abord ce dernier cas, et soit A un tableau du module. Les points de l'espace qui ont pour coordonnées relatives,

par rapport à A, des nombres entiers appartiennent au module, car ils sont formés, à partir des points de A, par addition et soustraction ([1]). En plus, ces points forment à eux seuls un module de dimension n, ce qui est évident si l'on considère leurs coordonnées relatives par rapport à A. Nous arrivons donc à cette conclusion, déjà indiquée à propos de la droite, les modules les plus simples de dimension n, dans un espace à n dimensions, sont formés des points $(p_1, p_2, \ldots, p_n)$ définis par

$$\| p_1 \quad p_2 \quad \ldots \quad p_n \| = \| x_1 \quad x_2 \quad \ldots \quad x_n \| \times A \qquad (x_i \text{ entiers}),$$

A étant un tableau quelconque ; il appartient d'ailleurs au module ainsi formé. On a un résultat analogue pour des modules de dimension m inférieure à celle de l'espace, il suffit de supposer que A est une matrice. D'une façon générale, nous dirons qu'*un module* $\mathfrak{M}$ *de dimension m dans un espace n est type*, *s'il existe une matrice* A *de type* (m, n) *et de rang m telle que tout point du module soit donné par l'égalité précédente. La matrice* A *sera dite une base du module.*

Il peut se faire que la définition d'un module déterminé ne mette pas en évidence immédiatement l'existence d'une base ; il est alors utile d'avoir un critérium pour reconnaître *a priori* si le module est type et un procédé, au moins théorique, pour former une base. C'est à quoi répondent l'énoncé et la démonstration suivants dont les applications ultérieures montreront l'importance ([2]).

Théorème. — *Pour qu'un module dans un espace à n dimensions soit type, il faut que les inégalités*

$$(2) \qquad |p_1| < \varepsilon, \quad |p_2| < \varepsilon, \quad \ldots, \quad |p_n| < \varepsilon$$

([1]) Dans le plan réel, par exemple, ceci revient à dire que si A et B, non en ligne droite avec l'origine, font partie d'un module, le quatrième sommet du parallélogramme construit sur OAB et tous les sommets du réseau qu'on en déduit, font partie du module.

([2]) Il ne suffit pas, en effet, d'avoir un critérium quelconque, mais, autant que possible, un critérium qui s'applique à d'autres exemples qu'à ceux qui ont été spécialement fabriqués pour en être des applications. Dans le cas présent, c'est le théorème qui a été fait en vue des applications; j'y ai été conduit, en effet, par la considération de propriétés diverses, dont les démonstrations présentaient des analogies manifestes (bases des entiers d'un corps, d'un idéal, des unités; périodes des fonctions, etc.).

ne soient vérifiées que par un nombre fini de points

$$(p_1, p_2, \ldots, p_n)$$

de 𝒜, quel que soit ε positif; il suffit qu'elles n'aient qu'un nombre fini de solutions pour un nombre ε positif donné.

Faisons d'abord quelques remarques au sujet de l'énoncé : d'après ce qui a été dit sur la continuité de la distance généralisée et la limitation du corps caractéristique, on peut remplacer les n inégalités précédentes par la seule inégalité

$$\text{(2 } bis) \qquad S(op) < \varepsilon,$$

S étant une distance généralisée quelconque. Il n'est même pas nécessaire que S vérifie toutes les conditions de M. Minkowski, et l'on peut évidemment remplacer la condition par celle qu'il y ait seulement un nombre fini de points de 𝒜 dans un domaine borné entourant l'origine; domaine, quelconque pour la condition nécessaire, choisi *a priori* pour la condition suffisante. Ceci montre, ce que prouvera d'ailleurs aussi la démonstration, que, dans l'énoncé, le choix des coordonnées absolues ou relatives est indifférent.

La condition est nécessaire : si, par rapport à une base A, tout point $(p_1, p_2, \ldots, p_n)$ de 𝒜 a pour coordonnées des nombres entiers $(x_1, x_2, \ldots, x_m)$, les x sont des fonctions linéaires et homogènes des p (premier Chapitre); les inégalités (2) entraînent, par suite, en désignant par G une limite supérieure des coefficients des fonctions linéaires

$$|x_i| < mG\varepsilon \qquad (i = 1, 2, \ldots, m)$$

et ces nouvelles égalités ne sont vérifiées, quel que soit ε, que par un nombre fini de systèmes d'entiers, c'est-à-dire de points de 𝒜.

Pour montrer que la condition est suffisante, établissons d'abord que, si elle est vérifiée pour un nombre donné ε, elle l'est aussi pour tout autre nombre ε′. Ceci est évident pour ε′ inférieur à ε, vérifions-le pour $k\varepsilon$, k étant un entier. Supposons l'espace réel et considérons les $(2k)^n$ points

$$(e_1\varepsilon, e_2\varepsilon, \ldots, e_n\varepsilon),$$
$$(-k < e_i \leq k, \quad e_i \text{ entier}):$$

tout point vérifiant les inégalités $|p_i| < k\varepsilon$ vérifie l'un des $(2k)^n$ systèmes

$$0 \leqq p_1 - e_1\varepsilon < \varepsilon, \quad 0 \leqq p_2 - e_2\varepsilon < \varepsilon, \quad \ldots, \quad 0 \leqq p_n - e_n\varepsilon < \varepsilon;$$

il suffit de prendre pour e_i *la partie entière* (1) de $\frac{p_i}{\varepsilon}$ qui est comprise entre $-k$ inclus et k exclus. Or, si nous considérons les points de $\mathcal{A}$, s'ils existent, vérifiant l'un de ces systèmes, leurs différences avec l'un d'entre eux sont encore des points de $\mathcal{A}$, dont les coordonnées sont, en valeur absolue, inférieures à ε; il en résulte que ces différences et, par suite, les points eux-mêmes, sont en nombre fini. Il n'y a donc aussi qu'un nombre fini de points vérifiant les $(2k)^n$ systèmes et, *a fortiori* (2), les inégalités proposées. La propriété est donc vraie pour tout nombre inférieur à $k\varepsilon$, c'est-à-dire pour un nombre quelconque. Si l'espace est semi-réel, par exemple $(p_1 + ip_2, p_1 - ip_2, p_3)$, les inégalités (1) n'ayant qu'un nombre fini de solutions, il en est *a fortiori* de même de

$$|p_1| < \frac{\varepsilon}{\sqrt{2}}, \quad |p_2| < \frac{\varepsilon}{\sqrt{2}}, \quad |p_3| < \frac{\varepsilon}{\sqrt{2}}.$$

Mais les points (p_1, p_2, p_3) forment un module réel et, d'après ce qui précède, il n'y a qu'un nombre fini de ces points vérifiant

$$|p_1| < \varepsilon', \quad |p_2| < \varepsilon', \quad |p_3| < \varepsilon',$$

quel que soit ε', donc un nombre fini de points de $\mathcal{A}$ vérifiant

$$|p_1 + ip_2| < \varepsilon'\sqrt{2}, \quad |p_3| < \varepsilon';$$

on voit sans peine que la démonstration est générale.

Ce premier point acquis, considérons les coordonnées relatives $(y_1, y_2, \ldots, y_m)$ des points de $\mathcal{A}$ relativement à une matrice du

(1) Rappelons que la partie entière est l'entier immédiatement inférieur, ou égal, au nombre.

(2) Il faut mettre *a fortiori*, car les points des $(2k)^n$ systèmes ne vérifient pas toutes les inégalités. Ceci, ainsi que la démonstration, sera illustré par un exemple géométrique. Dans le plan, les n inégalités primitives peuvent s'interpréter par le fait que le point (p_1, p_2) est intérieur, périmètre non compris, à un carré de côté $2k\varepsilon$. Remplacer cette condition par les $(2k)^2$ systèmes revient à diviser le carré en carrés de côté ε. Mais on ajoute ainsi au domaine le demi-périmètre du carré, au-dessous et à gauche de l'origine.

sous-espace contenant $\mathcal{A}$ (tableau, si $\mathcal{A}$ est de dimension n). Les inégalités $|y_i| < \varepsilon$ entraînent des inégalités analogues pour les coordonnées absolues $|p_i| < ng\varepsilon$, g étant le maximum des valeurs absolues des termes de la matrice; elles ne sont donc aussi vérifiées que par un nombre fini de points de $\mathcal{A}$. Nous allons maintenant supposer que la matrice est formée de m points du module $A_1, A_2, \ldots, A_m$ et raisonner sur le module $\mathcal{B}$ formé des points $(y_1, y_2, \ldots, y_m)$: $\mathcal{B}$ comprend les points $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, ... Considérons les points de $\mathcal{B}$ vérifiant les conditions

$$0 < y_1 \leqq 1, \qquad y_2 = y_3 = \ldots = y_m = 0,$$

ce sont des points du sous-espace de dimension 1 défini par l'origine et le point A_1. Ces points, ayant des coordonnées de valeur absolue inférieure à 1, sont en nombre fini; il en existe au moins un qui est $(1, 0, \ldots, 0)$. On peut donc choisir parmi eux celui pour lequel y_1 est le plus petit, soit $(a_1, 0, 0, \ldots, 0)$; ce point est bien déterminé. Considérons alors les points de $\mathcal{B}$ vérifiant

$$0 \leqq y_1 < a_1, \qquad 0 < y_2 \leqq 1, \qquad y_3 = \ldots = y_m = 0;$$

ce sont des points du sous-espace de dimension 2 défini par A, A_1, A_2. Le même raisonnement est toujours valable, il y a au moins un point $(0, 1, 0, \ldots, 0)$ vérifiant les conditions et il n'y en a qu'un nombre fini : on peut donc choisir celui pour lequel y_2 est le plus petit, soit

$$(b_1, b_2, 0, \ldots, 0).$$

Ce point est encore unique, car s'il en existait un second $(b'_1, b'_2, 0, \ldots, 0)$, nécessairement $b'_2 = b_2$, et, en supposant $b'_1 > b_1$, le point

$$(b'_1, b'_2, 0, \ldots) - (b_1, b_2, 0, \ldots) = (b'_1 - b_1, 0, \ldots)$$

appartiendrait encore à $\mathcal{B}$, sa première coordonnée serait positive et inférieure à a_1, ce qui est absurde, si elle n'est pas nulle. En considérant les conditions

$$0 \leqq y_1 < a_1, \qquad 0 \leqq y_2 < a_2, \qquad 0 < y_3 \leqq 1, \qquad y_4 = \ldots = y_m = 0,$$

on peut choisir un point $(c_1, c_2, c_3, 0, \ldots)$ et ainsi de suite, jus-

qu'à obtenir m points formant un tableau d'ordre m

$$B = \begin{Vmatrix} a_1 & 0 & 0 & \dots & 0 \\ b_1 & b_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ l_1 & l_2 & l_3 & \dots & l_m \end{Vmatrix}$$

$$\Delta(B) = a_1 b_2 \dots l_m \neq 0.$$

Donc B est un tableau de $\mathcal{M}$, le point de coordonnées

$$\| e_1 \quad e_2 \quad \dots \quad e_m \| \times B \qquad (e_i \text{ entiers})$$

appartient à $\mathcal{M}$, et il en est de même de sa différence avec un point quelconque de $\mathcal{M}$

$$\| z_1 \quad \dots \quad z_m \| = \| y_1 \quad \dots \quad y_m \| - \| e_1 \quad \dots \quad e_m \| \times B.$$

$$\begin{cases} y_1 - e_1 a_1 - e_2 b_1 - \dots \dots - e_m l_1 = z_1, \\ y_2 \qquad\quad - e_2 b_2 - \dots \dots - e_m l_2 = z_2, \\ \dots \dots \dots \dots \dots \dots \dots \dots, \\ y_{m-1} \qquad\qquad - e_{m-1} k_{m-1} - e_m l_{m-1} = z_{m-1}, \\ y_m \qquad\qquad\qquad\qquad - e_m l_m = z_m. \end{cases}$$

Déterminons successivement les entiers e_m, e_{m-1}, ..., e_1 par les conditions

$$0 \leqq \frac{y_m}{l_m} - e_m < 1,$$

$$0 \leqq \frac{y_{m-1} - e_m l_{m-1}}{k_{m-1}} - e_{m-1} < 1,$$

$$\dots \dots \dots \dots \dots \dots \dots \dots$$

$$0 \leqq \frac{y_1 - e_m l_1 - e_{m-1} k_1 - \dots - e_2 b_1}{a_1} - e_1 < 1,$$

c'est-à-dire prenons les parties entières des fractions successivement constituées. Mais alors, en tenant compte du fait que les a_1, b_2, ..., l_m sont positifs, on voit que les z vérifient les inégalités

$$0 \leqq z_1 < a_1, \qquad 0 \leqq z_2 < b_2, \qquad \dots, \qquad 0 \leqq z_{m-1} < k_{m-1}, \qquad 0 \leqq z_m < l_m.$$

Si l'on omet la dernière inégalité, on a les conditions qui ont servi à définir la dernière ligne de B; mais l_m ayant été choisi le plus petit possible, il est impossible que z_m lui soit inférieur; il est donc nul. Dans les $n - 1$ inégalités restantes, en omettant la der-

mière et en comparant aux conditions de définition de l'avant-dernière ligne de B, on montre de même que z_{m-1} est nul. Et ainsi de suite, tous les z sont nuls; donc, tout point de $\mathcal{B}$ a des coordonnées de la forme

$$\| x_1 \quad x_2 \quad \ldots \quad x_n \| = \| c_1 \quad c_2 \quad \ldots \quad c_m \| \times B,$$

ce qui prouve que B est une base de $\mathcal{B}$, qui est type. Il en resulte que $\mathcal{A}$ est aussi type, et $B \times M$ en est une base, en désignant par M la matrice de $\mathcal{A}$ choisie pour définir $\mathcal{B}$. Il est à remarquer que la démonstration précédente fournit un moyen, au moins théorique, de déduire de toute matrice M du module une base bien déterminée.

De la propriété générale ainsi démontrée, résulte une conséquence négative assez importante : *Si un module dans un espace à n dimensions n'est pas type, il y a une infinité de ses points vérifiant les inégalités*

$$|p_1| < \varepsilon, \quad |p_2| < \varepsilon, \quad \ldots, \quad |p_n| < \varepsilon$$

ou

$$|p_1 - \omega_1| < \varepsilon, \quad |p_2 - \omega_2| < \varepsilon, \quad \ldots, \quad |p_n - \omega_n| < \varepsilon$$

$(\omega_1, \ldots, \omega_n)$ étant un point quelconque du module.

C'est ce qui se produit, en particulier, pour un module de points $\mathcal{A}$ sur une droite, isomorphe holoédriquement d'un module type de points de dimension 2. (Pour avoir une telle correspondance, il suffit, comme dans l'exemple cité, de projeter les sommets d'un réseau de parallélogrammes sur une droite convenablement choisie.) Il y a alors une infinité de points de $\mathcal{A}$ dans tout intervalle $(-\varepsilon, +\varepsilon)$ entourant l'origine ; il en est aussi de même pour tout intervalle $(\alpha, \alpha + \eta)$ de la droite ; car si a est un point, ou un nombre, de $\mathcal{A}$ compris entre $-\frac{\eta}{3}$ et $+\frac{\eta}{3}$, il existe trois points $(\lambda-1)a$, λa, $(\lambda+1)a$, de $\mathcal{A}$ (λ entier) compris, au sens large, dans l'intervalle $(\alpha, \alpha + \eta)$; d'autre part, il y a une infinité de points de $\mathcal{A}$ distants de λa de moins de $|a|$ et, par conséquent, compris dans l'intervalle. Les points de $\mathcal{A}$ forment un ensemble *partout dense* [1] sur la droite.

[1] Il n'en est pas nécessairement de même pour un module type dans un plan, même de dimension 2 : on le constate aisément en considérant le module formé par les points ayant pour abscisses les nombres entiers et pour ordonnées les nombres rationnels (*voir* la Note I).

Considérons encore un nombre irrationnel a et le module de nombres

$$xa - y \qquad (x, y \text{ entiers}).$$

Les nombres de ce module, comprenant a et 1, ne peuvent être de la forme $k\alpha$ et le module n'est pas type. On peut donc trouver une infinité d'entiers x, y tels que

$$|xa - y| < \varepsilon \qquad \text{ou} \qquad \left| a - \frac{y}{x} \right| < \frac{\varepsilon}{|x|}.$$

C'est dire qu'on peut trouver une infinité de fractions $\frac{y}{x}$ s'approchant d'un nombre irrationnel donné de moins de $\frac{\varepsilon}{|x|}$. C'est un cas particulier d'une propriété trouvée primitivement dans la théorie des fractions continues et démontrée ensuite par Dirichlet ([1]). En considérant a comme l'abscisse d'un point sur une droite, on retrouve l'exemple précédent; on peut encore considérer a comme une abscisse curviligne sur un cercle, la longueur de la circonférence étant l'unité. Les nombres $xa - y$ sont alors les abscisses des sommets de la ligne brisée régulière d'angle au centre a; ces sommets forment un ensemble partout dense sur le cercle.

Tableaux et matrices d'un module.

Reprenons l'étude directe d'un module type $\mathcal{A}$, en le supposant d'abord de même dimension que l'espace. Tout point de $\mathcal{A}$ s'obtient en multipliant une base A à gauche par une matrice de type $(1, n)$ formée d'entiers. Donc, tout tableau P du module, formé de n points de $\mathcal{A}$, s'obtient en multipliant A à gauche par un

---

([1]) Dirichlet démontre, en outre, qu'on peut trouver de telles fractions, x ne dépassant pas $\frac{1}{\varepsilon}$, ce qui revient encore à dire qu'on peut approcher de a de moins de $\frac{1}{x^2}$. Dans certaines applications, notamment pour les périodes de fonctions, la propriété ci-dessus peut remplacer celle de Dirichlet. On peut encore considérer la propriété de Dirichlet comme donnant, pour un module type déterminé, une limitation inférieure de ε suffisante pour qu'il y ait des points du module vérifiant les conditions (1). A ce point de vue, elle se généralise aisément en remplaçant (1) par (1 *bis*) et en prenant un espace de dimension quelconque; elle constitue alors l'un des théorèmes de M. Minkowski, que nous établirons plus loin. On pourra aussi comparer ceci avec un raisonnement de J. Tannery (*Introduction à la théorie des fonctions*, t. I, p. 38-39).

tableau à termes entiers

$$P = SA \quad \begin{cases} \Delta(S) \neq 0, \\ S \text{ à termes entiers.} \end{cases}$$

La condition $\Delta(S) \neq 0$ est nécessaire pour que P soit un véritable tableau. Parmi ces tableaux, il y en a en général (sauf pour $n = 1$) une infinité qui sont des bases ; ils sont donnés par la propriété :

L'ensemble des bases d'un module type est identique à l'ensemble des tableaux équivalents à l'une d'elles, ou encore *forme un système de tableaux.*

Si A_1 et A sont deux bases, A_1 est un tableau du module de base A, donc

$$A_1 = SA \qquad \text{et} \qquad A = S^{-1}A_1,$$

mais A est aussi un tableau du module de base A_1, donc S^{-1} doit être à termes entiers, ce qui exige que S soit modulaire. Réciproquement tout point de $\mathcal{A}$ a, par rapport à une base A, des coordonnées relatives entières $(x_1, x_2, \ldots, x_n)$; par rapport à un tableau équivalent SA, il a pour coordonnées $(y_1, y_2, \ldots, y_n)$ définies par

$$\|y_1 \quad y_2 \quad \ldots \quad y_n\| \cdot SA = \|x_1 \quad x_2 \quad \ldots \quad x_n\| \cdot A$$

ou

$$\|y_1 \quad y_2 \quad \ldots \quad y_n\| = \|x_1 \quad x_2 \quad \ldots \quad x_n\| \cdot S^{-1};$$

S^{-1} étant à termes entiers, les y sont encore des nombres [1] entiers.

De ceci on déduit notamment qu'on peut, dans une base, changer l'ordre des lignes, ce qui était d'ailleurs évident *a priori*. Le déterminant d'un tableau du module est un multiple de $\Delta(A)$ et ne lui est égal, au signe près, que si ce tableau est lui-même une base. On peut donc encore dire que les bases d'un module *sont les tableaux de déterminant minimum* [2].

Pour un module type quelconque de dimension $m < n$, toute

---

(1) Cette démonstration ne diffère pas essentiellement de celle qui montre qu'une substitution modulaire transforme un système d'entiers en un système d'entiers et réciproquement.

(2) Dans le cas $n = 1$, la base est unique au signe près ; dans le cas $n = 2$, si l'on suppose que le plan représente une variable complexe, on a la propriété connue des systèmes de périodes d'une fonction elliptique.

matrice P du module se déduit encore d'une matrice de base A par l'égalité

$$P = SA \qquad (S \text{ à termes entiers});$$

cette égalité en entraîne C_n^m analogues entre les mineurs d'ordre m de A et les mineurs correspondants de P; il faut donc toujours $\Delta(S) \neq 0$ pour que P soit effectivement de rang m. On obtient encore les matrices de base en multipliant l'une d'elles à gauche par tous les tableaux modulaires d'ordre m. Enfin, la propriété du déterminant peut s'étendre en considérant les C_n^m déterminants des mineurs déduits de A.

La question des tableaux ou des matrices est liée à celle des *sous-modules;* nous appellerons ainsi tout module $\mathcal{B}$ dont les points font tous partie du module donné $\mathcal{A}$. Si $\mathcal{A}$ est type, il en est de même de tout sous-module $\mathcal{B}$, car $\mathcal{B}$ n'a *a fortiori* qu'un nombre fini de points au voisinage de l'origine. Si $\mathcal{B}$ est de même dimension que $\mathcal{A}$, sa base est un tableau ou une matrice de $\mathcal{A}$, donc de la forme SA. S'il est de dimension $m_1 < m$, sa base est de la même forme, mais S est une matrice à termes entiers de type (m_1, m); la condition $\Delta(S) \neq 0$ est remplacée cette fois par celle que S soit de rang m_1; on le vérifie sans difficulté en remarquant que les lignes de S sont les coordonnées relatives de certains points du sous-module par rapport à la matrice A.

Si l'on considère un sous-espace de dimension m passant par l'origine, il peut se faire qu'il ne contienne aucun point de $\mathcal{A}$, ou encore que tous les points de $\mathcal{A}$ qui y sont contenus appartiennent à un sous-espace de dimension moindre. Mais si l'on a pu s'assurer *a priori* qu'il existe dans ce sous-espace m_1 points de $\mathcal{A}$ formant une matrice de rang m_1, par exemple si l'on a défini le sous-espace par un tel système de m_1 points [1], tous les points de $\mathcal{A}$ situés dans ce sous-espace forment un sous-module type $\mathcal{B}$ de dimension m_1, et tous les autres sous-modules qui y sont situés sont des sous-modules de $\mathcal{B}$.

Ces notions permettent d'expliciter la marche suivie dans la démonstration du théorème fondamental et en même temps de

---

[1] Dans l'espace à 3 dimensions réel, par exemple, il suffit de considérer tous les points de $\mathcal{A}$ dans un plan passant par o et 2 points de $\mathcal{A}$ non en ligne droite avec o, ou les points sur une droite passant par o et un point de $\mathcal{A}$.

préciser la latitude possible dans le choix d'une base. Nous avons choisi d'abord une matrice arbitraire M (de rang m) de $\mathcal{A}$ et envisagé les points des sous-espaces de dimension 1, 2, ..., m définis par ox_1, ox_1x_2, ... Les points de $\mathcal{A}$ situés dans ces sous-espaces forment des sous-modules types $\mathcal{A}_1$, $\mathcal{A}_2$, ...; chacun d'eux contient le précédent et le dernier $\mathcal{A}_m$ est identique à $\mathcal{A}$. Ceci posé, examinons comment on obtient les m_1 premières lignes de la base $B \times M$; il suffit de multiplier la matrice formée des m_1 premières lignes de B par M; mais cette matrice a ses $m - m_1$ dernières colonnes formées de zéro; il suffit donc, finalement, de multiplier le mineur B_{m_1} formé des m_1 premières lignes et colonnes de B par la matrice M_{m_1} formée des m_1 premières lignes de M. D'autre part, dans les raisonnements faits pour déterminer les lignes de B_{m_1} on ne s'est servi que des points de $\mathcal{A}$ appartenant au sous-espace défini par les lignes de M_{m_1}, c'est-à-dire des points de $\mathcal{A}_{m_1}$. On peut donc recommencer sur $B_{m_1} \times M_{m_1}$ le raisonnement fait sur $B \times M$, et cette matrice est une base de $\mathcal{A}_{m_1}$. Donc, la marche suivie consiste à déterminer successivement des bases des sous-modules $\mathcal{A}_1$, $\mathcal{A}_2$, ..., $\mathcal{A}_m$. L'intérêt de cette méthode est que chacune de ces bases est obtenue de façon unique en ajoutant une ligne convenablement déterminée à la précédente [1]. On peut encore exprimer ce résultat : *on peut prendre pour m_1 premières lignes, et par suite pour m_1 lignes quelconques, d'une base, m_1 points du module formant une matrice de rang m_1, pourvu que cette matrice soit la base du sous-module de dimension m_1 formé par les points du module contenus dans le sous-espace qu'elle définit.*

Modules finis.

Les modules types sont, comme nous l'avons dit, les plus simples et tout autre module $\mathfrak{M}$ de dimension m admet comme sous-modules les modules types ayant pour bases les tableaux de $\mathfrak{M}$; il est donc nécessaire d'avoir plus de m points pour constituer $\mathfrak{M}$ par seule addition et soustraction. On pourrait citer

---

[1] On peut rapprocher cette manière de faire de la suite de composition d'un groupe.

après les modules types les modules de dimension m, qui peuvent se construire à partir d'un nombre fini p de points, p étant supposé supérieur à m ; soit

$$(a_1^i, a_2^i, \ldots, a_n^i) \qquad (i = 1, 2, \ldots, p).$$

Un tel module, que nous appellerons *fini et d'ordre* p, *est isomorphe holoédriquement à un module type* $\mathfrak{L}$ *de dimension* p ; on peut, en supposant par exemple que la matrice formée par les m premiers points A_i est de rang m, prendre comme base de $\mathfrak{L}$ la matrice

$$\begin{Vmatrix} a_1^1 & a_2^1 & \ldots & a_n^1 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & . & . & \ldots & . \\ a_1^m & a_2^m & \ldots & a_n^m & 0 & 0 & \ldots & 0 \\ a_1^{m+1} & a_2^{m+1} & \ldots & a_n^{m+1} & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & . & . & \ldots & . \\ a_1^p & a_2^p & \ldots & a_n^p & 0 & 0 & \ldots & 1 \end{Vmatrix},$$

de type $(p, n+p-m)$ et de rang p. On vérifie sans peine que l'isomorphisme est holoédrique.

D'une façon pour ainsi dire réciproque, on peut, d'un module type, déduire des modules finis isomorphes, par *projection* sur un sous-espace. Considérons, pour fixer les idées, un module type $\mathcal{A}$ de dimension n dans un espace de même dimension, de base A et formé des points $(p_1, p_2, \ldots, p_n)$; et une matrice P de type (n, m) et de rang m. L'ensemble des points d'un espace à m dimensions

$$\| z_1 \quad z_2 \quad \ldots \quad z_m \| = \| p_1 \quad p_2 \quad \ldots \quad p_n \| \times \mathrm{P},$$

forme un module $\mathfrak{L}$ de dimension m (puisque AP est de rang m), isomorphe à $\mathcal{A}$. Pour que l'isomorphisme soit holoédrique, il faut et il suffit qu'au point nul de $\mathfrak{L}$ corresponde le seul point nul de $\mathcal{A}$. La condition est évidemment nécessaire; si elle est remplie, à deux points distincts de $\mathcal{A}$ ne peut correspondre un même point de $\mathfrak{L}$, sinon, à leur différence qui n'est pas nulle, correspondrait le point nul [1] de $\mathfrak{L}$. Cette condition est équivalente à celle *qu'il*

---

[1] Ce raisonnement est général et s'appliquerait à l'isomorphisme de deux modules quelconques.

n'y ait pas une même relation linéaire et homogène à coefficients entiers entre les termes des colonnes de AP.

En particulier, considérons les points d'un espace à m dimensions dont les coordonnées sont les m premières coordonnées des points de $\mathcal{A}$ et le module $\mathfrak{P}$ qu'ils forment; alors

$$\mathrm{P} = \left\| \begin{matrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ . & . & \ldots & . \\ 0 & 0 & \ldots & 1 \\ 0 & 0 & \ldots & 0 \\ . & . & \ldots & . \\ 0 & 0 & \ldots & 0 \end{matrix} \right\| \begin{matrix} \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\} m. \\ \left.\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right\} n-m. \end{matrix}$$

et AP est formée des m premières colonnes de A; pour que $\mathfrak{P}$ soit isomorphe holoédriquement à $\mathcal{A}$, il faut et il suffit qu'il n'y ait pas une même relation linéaire et homogène à coefficients entiers entre les termes de ces m colonnes; s'il en est ainsi, d'après la conséquence négative du théorème fondamental, il y a une infinité de points de $\mathfrak{P}$ ou de $\mathcal{A}$ vérifiant

$$|p_1| < \varepsilon, \quad |p_2| < \varepsilon, \quad \ldots, \quad |p_m| < \varepsilon.$$

L'étude des *modules infinis* semble encore à peine ébauchée, on peut y rattacher quelques questions actuellement assez complexes de la théorie des nombres et dont les démonstrations, quoique jolies, ne semblent guère susceptibles d'extension. L'existence d'une infinité de nombres premiers peut se traduire en disant que le module formé par les logarithmes des nombres rationnels positifs est infini; la transcendance de e se traduit aussi par l'infinitude du module de nombres formé par e et toutes ses puissances entières.

Examinons seulement, parmi les modules infinis, les modules de points d'un espace à n dimensions dont les coordonnées relatives à un tableau A sont tous les systèmes de n nombres rationnels; ils sont désignés par M. Esclangon sous le nom de *corps de périodes;* nous rencontrerons, d'ailleurs, ultérieurement une autre raison de cette dénomination. Le tableau A peut encore s'appeler *une base; toutes les bases d'un corps de périodes se déduisent*

de l'une d'elles en la multipliant à gauche par tous les tableaux à termes rationnels de déterminant non nul. Car dans l'égalité

$$\| x_1 \ x_2 \ \dots \ x_n \| \times A = \| y_1 \ y_2 \ \dots \ y_n \| \times SA \qquad (\text{S à termes rationnels}),$$

à tout système de x rationnels correspond un et un seul système de y rationnels et réciproquement; en outre, pour qu'il en soit ainsi, il faut évidemment que S soit à termes rationnels.

CHAPITRE III.

ENTIERS ET SYSTÈMES D'ENTIERS.

Dans les Chapitres précédents, nous n'avons utilisé parmi les propriétés particulières aux entiers que la seule notion de *partie entière* d'un nombre quelconque, qui se confond avec celle de *quotient à une unité près* si le nombre est une fraction. Nous allons montrer d'abord comment les principes généraux de la théorie des modules permettent de retrouver les principales propriétés connues de la divisibilité des entiers et certains résultats plus récents de la théorie des équations indéterminées ([1]).

Divisibilité.

Une première remarque immédiate, mais fondamentale, est que si un module de nombres est formé uniquement d'entiers, il est nécessairement type, puisqu'il n'a pas d'éléments infiniment petits (ou voisins de l'origine); il est donc identique à l'ensemble des multiples d'un entier a, c'est-à-dire à tous les nombres xa, x étant un entier quelconque, positif, négatif ou nul.

Proposons-nous d'abord de trouver l'ensemble des multiples communs à plusieurs entiers a, b, ..., l. Cet ensemble forme un module $\mathfrak{M}$, la différence ou la somme de deux multiples communs étant encore un multiple commun. Donc il est formé par tous les

---

([1]) On trouvera ces résultats exposés à un point de vue différent dans l'*Essai sur la théorie des nombres* de T.-J. STIELTJES (Premiers éléments). Stieltjes y donne aussi certains résultats de M. Smith, qui ne seront pas traités ici et qui se rattachent plutôt à l'équivalence des formes quadratiques et bilinéaires, multiplication d'un tableau à droite et à gauche par des tableaux modulaires symétriques ou même indépendants (*cf.* Chapitre I, note de la page 11).

multiples [1] d'un nombre μ qui est par conséquent *le plus petit des multiples communs* des nombres $a, b, \ldots, l$. Nous emploierons pour représenter ce plus petit multiple commun la notation de T.-J. Stieltjes

$$\mu = |a, b, \ldots, l|.$$

Cette propriété du plus petit multiple commun permet de trouver celle du plus grand commun diviseur en cherchant les multiples communs des diviseurs communs. Mais on peut aussi procéder directement; soient des entiers $a, b, \ldots$, peut être en nombre infini, et considérons le module $\mathfrak{D}$ de nombres formé à partir de ceux-là par addition et soustraction. *C'est l'ensemble des nombres*

$$xa + yb + \ldots \qquad (x, y, \ldots \text{ entiers quelconques}),$$

il est identique à l'ensemble des multiples d'un certain nombre δ qui, appartenant au module, peut être mis sous la forme précédente

$$\delta = ua + vb + \ldots.$$

Tous les diviseurs communs de $a, b, \ldots$ sont des diviseurs de tous les nombres de $\mathfrak{D}$, donc de δ et réciproquement. Nous emploierons encore pour représenter δ qui est le *plus grand des diviseurs communs* de $a, b, \ldots$, la notation de Stieltjes

$$(a, b, \ldots).$$

Toutefois, nous emploierons cette expression indifféremment, soit pour représenter δ lui-même, soit pour représenter l'ensemble des multiples de δ, c'est-à-dire $\mathfrak{D}$. Si $\delta = 1$ ($\mathfrak{D}$ identique à l'ensemble des entiers), les nombres $a, b, \ldots$ sont dits *premiers entre eux* dans leur ensemble.

Nous avons établi l'existence de μ et δ sans donner de méthode pratique pour les déterminer. Pour trouver le plus grand commun diviseur d'un nombre fini de nombres $a, b, \ldots, l$, re-

---

(1) Si l'on incorpore à cette démonstration celle du théorème sur les modules types appliquée à ce cas particulier, on obtient la démonstration donnée par Stieltjes (*loc. cit.*). Il est à remarquer qu'on se sert ainsi de l'*algorithme de la division*.

marquons d'abord que dans l'expression $(a, b, \ldots, l)$ on peut permuter les nombres d'une façon quelconque et supposer par conséquent que l est le plus petit d'entre eux. L'algorithme d'Euclide pour la recherche de δ se déduit alors de l'égalité manifeste

$$(a, b, \ldots, l) = (a - ql, b - q'l, \ldots, l).$$

Si $q, q', \ldots$ sont les quotients de $a, b, \ldots$ par l on définit ainsi $\mathfrak{D}$ par des nombres inférieurs aux précédents. En appliquant le même procédé avec le plus petit des nombres de la deuxième parenthèse et ainsi de suite, on définit finalement $\mathfrak{D}$ par un seul nombre δ (qui est le plus grand commun diviseur cherché) et des o. Il est à remarquer que cette méthode donne en même temps l'expression de δ comme terme de $\mathfrak{D}$ (théorème de Bezout). Il n'était pas sans intérêt de rappeler cet algorithme, car c'est à lui que se ramène finalement la résolution pratique des problèmes que nous traiterons dans la suite de ce Chapitre.

Les démonstrations et propriétés précédentes sont encore valables pour la recherche des multiples et diviseurs communs à plusieurs fractions supposées toutefois en nombre fini. Il suffit de remarquer que les éléments des modules $\mathfrak{M}$ et $\mathfrak{D}$ sont des fractions dont le dénominateur est limité supérieurement. L'algorithme d'Euclide s'étend également, en remplaçant dans l'énoncé le quotient de a par l par la partie entière de $\frac{a}{l}$.

Les diverses propriétés de la divisibilité des entiers et notamment la recherche du plus petit multiple commun peuvent se déduire de l'existence ainsi établie du plus grand commun diviseur et du plus petit multiple commun; il est bon d'y ajouter les propriétés immédiates, vraies pour un nombre quelconque d'entiers

$$(1) \quad \begin{cases} [a, b, c] = [[a, b], c], \\ (a, b, c) = ((a, b), c), \end{cases}$$

$$(2) \quad \begin{cases} [\lambda a, \lambda b, \lambda c] = \lambda [a, b, c] \\ (\lambda a, \lambda b, \lambda c) = \lambda (a, b, c) \end{cases} \qquad (\lambda \text{ entier}),$$

et aussi, puisque l'existence de μ et de δ a été établie indépendamment, la propriété qui peut servir de lien entre eux : *la*

condition nécessaire et suffisante pour que μ soit le plus petit multiple commun de $a, b, c, \ldots,$ est que $\frac{\mu}{a}, \frac{\mu}{b}, \cdots$ soient des entiers premiers entre eux (¹).

Car si μ est le plus petit multiple commun, on ne peut avoir

$$\left(\frac{\mu}{a}, \frac{\mu}{b}, \cdots\right) = \alpha > 1,$$

sinon $\frac{\mu}{\alpha}$ serait un multiple commun inférieur à μ; en outre, si la condition est remplie pour μ, pour tout autre multiple commun $\mu' = \lambda\mu$ on a

$$\left(\frac{\mu'}{a}, \frac{\mu'}{b}, \cdots\right) = \lambda\left(\frac{\mu}{a}, \frac{\mu}{b}, \cdots\right) = \lambda > 1.$$

Citons quelques conséquences de ces principes, d'abord l'expression du plus petit multiple commun :

(3) $$|a, b, c| = \frac{abc}{(ab, bc, ca)};$$

il suffit de constater, ce qui est immédiat, que les quotients du deuxième membre par a, b, c sont premiers entre eux. Soit encore la propriété considérée parfois comme fondamentale et dont se servent la plupart des auteurs de Traités d'arithmétique pour établir l'existence et l'expression du plus petit multiple commun, *si λ et b sont premiers entre eux* (²),

$$(a\lambda, b) = (a, b).$$

La démonstration peut se résumer par la suite d'égalités

$$(a\lambda, b) = (a\lambda, ab, b) = ((a\lambda, ab), b) = (a(\lambda, b), b) = (a, b).$$

Indiquons enfin une dernière propriété moins connue, dont on peut trouver de nombreuses modifications

(4) $$|(a, d), (b, d), (c, d)| = (|a, b, c|, d).$$

(¹) La propriété analogue pour le plus grand commun diviseur est plus immédiate mais moins utile, car on peut la considérer comme un simple cas particulier de la deuxième des égalités (2).

(²) On l'énonce habituellement en supposant $(a\lambda, b) = b$; si un nombre divise un produit de deux facteurs, et qu'il est premier avec l'un d'eux, il divise l'autre.

Posons

$$\alpha = (a, d), \quad \beta = (b, d), \quad \gamma = (c, d)$$

et considérons les quotients du deuxième membre par ces trois nombres

$$\frac{1}{\alpha}(|a, b, c|, d) = \left(\frac{a}{\alpha}\,\frac{|a, b, c|}{a}, \frac{d}{\alpha}\right) = \left(\frac{|a, b, c|}{a}, \frac{d}{\alpha}\right),$$

la dernière égalité étant obtenue en appliquant le principe précédent, puisque $\frac{a}{\alpha}$ et $\frac{d}{\alpha}$ sont premiers entre eux. Chacun des quotients ainsi obtenus est entier et leur plus grand commun diviseur est

$$\left(\left(\frac{|a, b, c|}{a}, \frac{d}{\alpha}\right), \ldots\right) = \left(\frac{|a, b, c|}{a}, \frac{|a, b, c|}{b}, \frac{|a, b, c|}{c}, \frac{d}{\alpha}\right)$$
$$= \left(1, \frac{d}{\alpha}\right) = 1.$$

Modules de points entiers.

Considérons maintenant, dans un espace à n dimensions, un module $\mathfrak{M}$ formé de points dont les n coordonnées sont respectivement des entiers. Les inégalités (2) du théorème fondamental n'ayant toujours qu'un nombre fini de solutions, un tel module est nécessairement type. C'est d'ailleurs un sous-module du module $\mathfrak{E}$ constitué par tous les points dont les coordonnées sont des nombres entiers.

Si $\mathfrak{M}$ est de dimension n, ses bases forment un système de tableaux d'ordre n à termes entiers. Pour $n > 1$, il y a une infinité de telles bases, mais on peut en distinguer une, d'une forme particulièrement remarquable. C'est ce qui résulte de l'important théorème dû à Hermite :

Un tableau à termes entiers T *est équivalent à un tableau et un seul de la forme*

$$(5) \qquad \mathrm{U} = \begin{Vmatrix} a_1^1 & 0 & 0 & \ldots & 0 \\ a_2^1 & a_2^2 & 0 & \ldots & 0 \\ \cdot\ \cdot & \cdot\ \cdot & \cdot & \ldots & \cdot \\ a_n^1 & a_n^2 & a_n^3 & \ldots & a_n^n \end{Vmatrix} \qquad (a_i^i > 0).$$

dont les termes vérifient les conditions

$$(5\ bis)\quad \left\{\begin{array}{llll} 0 \leq a_2^1 < a_1^1, & 0 \leq a_3^1 < a_1^1, & \dots\dots & 0 \leq a_n^1 < a_1^1, \\ & 0 \leq a_3^2 < a_2^2, & \dots\dots & 0 \leq a_n^2 < a_2^2, \\ & & \dots\dots & \dots\dots\dots\dots, \\ & & & 0 \leq a_n^{n-1} < a_{n-1}^{n-1}. \end{array}\right.$$

Un tel tableau sera dit mis sous la *forme réduite d'Hermite*.

Pour arriver à ce résultat nous allons procéder par cheminement en construisant à partir de T un tableau équivalent T′, à partir de T′ un tableau équivalent T″ et ainsi de suite; pour plus de simplicité nous désignerons les termes de ces différents tableaux toujours par a_i^j. Ceci convenu déduisons T′ de T par un changement de lignes, ce qui est une équivalence, de façon que dans T′, a_n^n soit le plus petit en valeur absolue des termes de la dernière colonne a_i^n. Déduisons T″ équivalent à T′ par l'égalité

$$T'' = \left\| \begin{array}{ccccc} 1 & 0 & \dots & 0 & -x_1 \\ . & . & \dots & . & \dots\dots \\ 0 & 0 & \dots & 1 & -x_{n-1} \\ 0 & 0 & \dots & 0 & \pm 1 \end{array} \right\| T';$$

le signe du dernier terme et les x étant choisis de façon que dans T″, a_n^n soit positif et tous les a_i^n positifs et inférieurs à a_n^n. Recommençons sur T″ les deux mêmes opérations que sur T et ainsi de suite; ceci revient à faire sur les entiers de la dernière colonne de T, les opérations du plus grand commun diviseur. On finit par avoir un tableau où les termes a_i^n sont nuls, excepté a_n^n qui est positif. En considérant dans ce nouveau tableau les n-1 termes de la $(n\text{-}1)^{\text{ième}}$ colonne, on peut recommencer les opérations précédentes, en permutant les n-1 premières lignes et multipliant à gauche par des tableaux :

$$\left\| \begin{array}{ccccc} 1 & 0 & \dots & -y_1 & 0 \\ 0 & 1 & \dots & -y_2 & 0 \\ . & . & \dots & \dots\dots & . \\ 0 & . & .. & \pm 1 & 0 \\ 0 & . & \dots & 0 & 1 \end{array} \right\|.$$

On peut ainsi annuler tous les termes de la $(n\text{-}1)^{\text{ième}}$ colonne audessus de la diagonale principale; de même pour la $(n\text{-}2)^{\text{ième}}$ co-

lonne, ..., jusqu'à la deuxième incluse : on obtient un tableau U de la forme (5).

Ceci acquis, cherchons les tableaux $U' = \Sigma U$ équivalents à U, donc à T, et de la forme (5). En désignant par α_i^j les termes de Σ et en développant les calculs, on constate d'abord sans difficulté qu'il est nécessaire que les α au-dessus de la diagonale principale (α_i^j, $i < j$) soient nuls. Mais on doit avoir, puisque Σ est unimodulaire,

$$\alpha_1^1 \alpha_2^2 \ldots \alpha_n^n = \Delta(\Sigma) = \pm 1 ;$$

les α_i^i étant des entiers sont donc tous égaux à ± 1 et même à $+1$, puisque dans U et U' les termes de la diagonale principale sont positifs. Ces conditions sont d'ailleurs suffisantes et, s'il en est ainsi, on trouve pour U' une expression de la forme

$$U' = \left\| \begin{matrix} a_1^1 & 0 & \ldots & 0 \\ a_2^1 + a_1^1 \alpha_2^1 & a_2^2 & \ldots & 0 \\ a_3^1 + a_2^1 \alpha_3^2 + a_1^1 \alpha_3^1 & a_3^2 + a_2^2 \alpha_3^2 & \ldots & 0 \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots & \ldots & . \\ a_n^1 + a_{n-1}^1 \alpha_n^{n-1} + \ldots + a_1^1 \alpha_n^1 & a_n^2 + a_{n-1}^2 \alpha_n^{n-1} + \ldots + a_2^2 \alpha_n^2 & \ldots & a_n^n \end{matrix} \right\| .$$

On peut alors déterminer successivement les entiers

$$\alpha_2^1, \quad \alpha_3^2, \quad \ldots, \quad \alpha_n^{n-1} ; \qquad \alpha_3^1, \quad \alpha_4^2, \quad \ldots, \quad \alpha_n^{n-2} ; \qquad \ldots ; \qquad \alpha_n^1,$$

de façon que les termes de U' vérifient les égalités (5 *bis*) et ceci n'est possible que d'une seule façon. Il faut pour cela faire des divisions par les a_i^i, c'est-à-dire encore chercher des *restes minima positifs, module* a_i^i. [On pourrait aussi chercher des restes minima absolus, c'est-à-dire faire vérifier aux termes de U' les conditions

$$(5\ ter) \qquad |a_i^j| \leq \frac{1}{2} a_i^i \qquad (i > j),$$

il y aurait alors ambiguïté de signe pour ceux des termes, s'ils existent, pour lesquels la condition précédente est une égalité [1].] Il est à remarquer que la démonstration ainsi faite constitue

---

[1] On pourrait aussi faire une permutation de lignes dans la forme (5) et définir par exemple, une forme réduite où les termes au-dessous de la diagonale principale seraient nuls.

une méthode pratique de recherche du tableau réduit d'Hermite.

Comme l'algorithme d'Euclide s'étend aux fractions, la propriété précédente s'étend au cas d'un tableau T à termes fractionnaires. Dans l'un ou l'autre cas on peut encore l'énoncer : *dans tout système de tableaux à termes entiers ou fractionnaires, il existe un et un seul tableau de la forme* (5) *et vérifiant les conditions* (5 *bis*). Ceci permet, notamment, de trouver tous les systèmes vérifiant certaines conditions, par exemple ayant un déterminant δ donné au signe près ; il suffit de chercher tous les tableaux réduits d'Hermite ayant δ pour déterminant. Si les termes sont entiers ou si leurs dénominateurs sont limités, on ne trouve ainsi qu'un nombre fini de tableaux, donc de systèmes ; car il n'y a qu'un nombre fini de façons de décomposer δ en un produit de facteurs (termes de la diagonale principale), les autres termes du tableau étant inférieurs à ceux-là, il n'y a choix, finalement, qu'entre un nombre fini d'arrangements ; il en est de même si δ est seulement limité supérieurement en valeur absolue.

Ce qui précède permet aussi de préciser quelle base particulière a été obtenue dans la démonstration du théorème fondamental sur les modules types. Une matrice M du module étant choisie, toute base est de la forme $B\times M$, B étant un tableau à termes fractionnaires (et même l'inverse d'un tableau à termes entiers), défini à une équivalence près. Dans la démonstration, on a choisi la base particulière pour laquelle B est de la forme réduite d'Hermite ; c'est ce qui résulte des conditions successives imposées aux termes de B.

Considérons encore un module quelconque $\mathfrak{M}$ de base A et un sous-module $\mathfrak{M}'$ de même dimension, donc de base $S\times A$, S étant un tableau d'ordre n à termes entiers, défini à une équivalence près ; le nombre entier $|\Delta(S)|$ étant bien défini, on peut se proposer de lui trouver une signification. Supposons S mis sous la forme réduite d'Hermite et soient $y_1, y_2, \ldots, y_m$ les coordonnées relatives d'un point quelconque de $\mathfrak{M}$ par rapport à A ; les y étant entiers et, étant donnée la forme de S, on peut toujours poser

$$\|y_1 \quad \ldots \quad y_m\| = \|z_1 \quad \ldots \quad z_m\| \times S + \|r_1 \quad \ldots \quad r_m\|$$

$$(z, r \text{ entiers}, \; 0 \leq r_i < a_i^i).$$

les r sont ainsi déterminés de façon unique [1]. Ceci posé, répartissons les points de $\mathfrak{M}$ par classes, en mettant dans une même classe des points dont la différence appartient à $\mathfrak{M}'$ (*congrus suivant le module* $\mathfrak{M}'$) : cette classification n'entraîne pas d'ambiguïté : deux points congrus à un troisième étant congrus entre eux (A-B, A-C étant dans $\mathfrak{M}'$, il en est de même de leur différence B-C). On vérifie aisément que, pour que deux points de $\mathfrak{M}$ soient dans une même classe, il faut et suffit qu'il leur corresponde les mêmes systèmes de r. *Il y a donc autant de classes que de systèmes de r différents* [2], *c'est-à-dire*

$$a_1^1 a_2^2 \dots a_m^m = |\Delta(\mathfrak{M}')|.$$

Examinons enfin le cas d'un module de points entiers dont la dimension n est inférieure à celle de l'espace. Sa base est une matrice de type (m, n) et de rang m ; elle n'est définie qu'à un produit près à gauche par un tableau unimodulaire, de sorte qu'on peut toujours amener un de ses mineurs d'ordre m (à déterminant non nul) à être de la forme réduite d'Hermite ; ce mineur étant choisi, cette réduction n'est possible que d'une seule manière.

Systèmes de formes.

Soit un système de m formes indépendantes à $n = m + p$ inconnues et à coefficients entiers

$$(1) \qquad \xi_i = a_i^1 x_1 + a_i^2 x_2 + \dots + a_i^n x_n \qquad (i = 1, 2, \dots, m),$$

la matrice A des coefficients de type (n, m) est de rang m.

D'un tel système on peut déduire divers modules de points entiers, soit, en considérant les valeurs de ces formes quand on donne aux x des valeurs entières, soit en considérant les valeurs des x qui annulent les ξ (*zéros du système*), soit encore en considérant les coefficients de ces formes et de toutes celles de leurs combinaisons linéaires qui ont des coefficients entiers. Nous allons étudier ces divers modules et leurs relations.

---

(1) λ_m et r_m sont le quotient et le reste de la division de y_m par a_m^m ; λ_{m-1} et r_{m-1} quotient et reste de la division de $y_{m-1} - \lambda_m a_m^{m-1}$ par a_{m-1}^{m-1} et ainsi de suite.

(2) Pour l'utilisation de cette propriété, *voir* la Note III.

L'ensemble des points $(\xi_1, \xi_2, \ldots, \xi_m)$, les x étant des entiers, forme, dans un espace de dimension m, un module type $\mathfrak{M}$; $\mathfrak{M}$ comprend les n points $(a_j^1, a_j^2, \ldots, a_j^m)$, il est donc de dimension m et l'on a

$$\|\xi_1 \quad \xi_2 \quad \ldots \quad \xi_m\| = \|\lambda_1 \quad \lambda_2 \quad \ldots \quad \lambda_m\| \times \mathrm{B},$$

$$\mathrm{B} = \begin{Vmatrix} c_1^1 & 0 & 0 & \ldots & 0 \\ c_2^1 & c_2^2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ c_m^1 & c_m^2 & c_m^3 & \ldots & c_m^m \end{Vmatrix}.$$

Pour trouver B à partir des coefficients des m formes et avoir les relations entre les x et les λ, il est commode de leur adjoindre p formes (¹), $\eta_1, \eta_2, \ldots, \eta_p$, à coefficients entiers, assujetties à la seule condition de former avec les premières un système de n formes indépendantes; on peut, par exemple, prendre

$$\eta_1 = x_1, \qquad \eta_2 = x_2, \qquad \ldots, \qquad \eta_p = x_p,$$

si le mineur formé par les m dernières lignes de la matrice des a a un déterminant non nul. Les points $(\eta_1, \ldots, \eta_p, \xi_1, \ldots, \xi_m)$ forment un module type $\mathfrak{M}'$ de dimension n dont une base est formée par les coefficients des formes, soit, dans l'exemple indiqué :

$$\mathrm{M}' = \begin{Vmatrix} 1 & 0 & \ldots & 0 & a_1^1 & a_1^2 & \ldots & a_1^m \\ 0 & 1 & \ldots & 0 & a_2^1 & a_2^2 & \ldots & a_2^m \\ \cdot & \cdot & \ldots & \cdot & \cdot\cdot & \cdot\cdot & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & a_p^1 & a_p^2 & \ldots & a_p^m \\ 0 & 0 & \ldots & 0 & a_{p+1}^1 & a_{p+1}^2 & \ldots & a_{p+1}^m \\ \cdot & \cdot & \ldots & \cdot & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & a_n^1 & a_n^2 & \ldots & a_n^m \end{Vmatrix},$$

on peut construire, par des opérations pratiquement réalisables, le tableau de la forme réduite d'Hermite $\mathrm{B}' = \mathrm{S} \times \mathrm{M}'$ équivalent à M'. Le mineur B formé par les m dernières lignes et colonnes de B' est aussi sous la forme réduite d'Hermite, et c'est la base cherchée. Le tableau modulaire S est tel que

$$\mathrm{S} \times \begin{Vmatrix} a_1^1 & \ldots & a_1^m \\ a_2^1 & \ldots & a_2^m \\ \ldots & \ldots & \ldots \\ a_n^1 & \ldots & a_n^m \end{Vmatrix} = \mathrm{S}^{-1} \times \begin{Vmatrix} 0 & \ldots & 0 \\ \cdot & \ldots & \cdot \\ 0 & \ldots & 0 \\ & \mathrm{B} & \end{Vmatrix}.$$

(¹) Si $p = 0$, les raisonnements sont valables *a fortiori*.

mais il est à remarquer qu'au seul point de vue de cette égalité S et S^{-1} ne sont pas entièrement déterminés : les p premières colonnes de S^{-1} dépendent seulement des formes y_i adjointes aux ξ.

La relation entre les x et les z peut s'obtenir en égalant les expressions des coordonnées des points de $\mathfrak{M}'$ à partir des deux bases M' et B'. On a ainsi

$$\| x_1 \quad \dots \quad x_n \| \times M' = \| y_1 \quad \dots \quad y_p \quad z_1 \quad \dots \quad z_m \| \times B'$$

et

$$\| x_1 \quad \dots \quad x_n \| = \| y_1 \quad \dots \quad y_p \quad z_1 \quad \dots \quad z_m \| \times S.$$

Donc, à tout système de z, c'est-à-dire à tout point déterminé de $\mathfrak{M}$ correspond, si $p > 0$, une infinité de valeurs des x dépendant de p indéterminées entières ; si $p = 0$, les x sont déterminés.

Indiquons encore quelques propriétés du nombre entier $|\Delta(B)|$; d'après les propriétés des tableaux d'un module, c'est le plus grand commun diviseur des déterminants, en nombre infini, des tableaux du module. On obtient de tels tableaux en prenant les mineurs non nuls déduits de la matrice A des a. Ces déterminants sont donc des multiples de $|\Delta(B)|$, mais on peut montrer en plus *que* $|\Delta(B)|$ *est le plus grand commun diviseur des mineurs de* A *ou, suivant une locution abrégée de Stieltjes, le plus grand commun diviseur de la matrice* A. En considérant la relation entre A, S^{-1} et B, on voit qu'on obtient le mineur formé des lignes de rang $i_1, i_2, \dots, i_m$ de A en multipliant B à gauche par le mineur d'ordre m de S^{-1} formé par les m dernières colonnes et les lignes de rang $i_1, i_2, \dots, i_m$. Donc, les quotients des déterminants de A par $\Delta(B)$ sont les déterminants des mineurs correspondants de la matrice formée par les m dernières colonnes de S^{-1}. Ces déterminants sont premiers entre eux dans leur ensemble, car, en appliquant la règle de Laplace pour le développement de $\Delta(S^{-1})$, on voit que le plus grand commun diviseur des dits déterminants doit diviser $|\Delta(S^{-1})|$ qui est égal à 1.

Module de zéros. — Changeant maintenant de point de vue, considérons, dans un espace à n dimensions, les systèmes de valeurs des variables x ; désignons toujours par $\mathcal{E}$ l'ensemble de tous les points à coordonnées entières de cet espace. Les équa-

tions

$$(6\ bis)\qquad \xi_1 = 0, \quad \xi_2 = 0, \quad \ldots, \quad \xi_m = 0$$

définissent un sous-espace de dimension $p = n - m$ contenant l'origine. Les coefficients des formes ξ étant rationnels, on peut choisir p solutions indépendantes du système précédent qui soient rationnelles et même entières. Donc, tous les points de $\mathcal{E}$ situés dans ce sous-espace, c'est-à-dire toutes les solutions entières des équations (6 *bis*), forment un module type $\mathcal{E}_p$ de dimension p. Le calcul précédemment fait pour les valeurs des ξ conduit à l'expression d'une base de $\mathcal{E}_p$; pour que les ξ soient nuls, il faut et il suffit que les λ soient nuls, ce qui donne pour les x les valeurs

$$\| x_1 \quad x_2 \quad \ldots \quad x_n \| = \| \mu_1 \quad \ldots \quad \mu_p \quad 0 \quad \ldots \quad 0 \| \times S$$

ou

$$\| x_1 \quad x_2 \quad \ldots \quad x_n \| = \| \mu_1 \quad \ldots \quad \mu_p \| \times P,$$

P *étant la matrice formée par les p premières lignes de* S; *cette matrice est une base de* $\mathcal{E}_p$. Les déterminants des mineurs de P sont, d'après la règle de Laplace, des entiers premiers entre eux [1]; il en est de même de toute autre base ΣP, les déterminants ayant au plus changé de signe [Σ d'ordre m, $\Delta(\Sigma) = \pm 1$].

Module rectangulaire. — Pour définir un sous-module de $\mathcal{E}$ de dimension inférieure à n, on peut encore définir le sous-espace qui le contient par un certain nombre de points entiers indépendants. Prenons pour cet effet les m points $(a_1^i, a_2^i, \ldots, a_n^i)$ dont les coordonnées sont les coefficients des ξ, on aura un système de $n - m = p$ équations indépendantes définissant ce sous-espace en prenant pour leurs coefficients p solutions indépendantes de (6 *bis*), notamment les lignes de P; soit

$$(7)\qquad \alpha_i^1 y_1 + \alpha_i^2 y_2 + \ldots + \alpha_i^n y_n = 0 \qquad (i = 1, 2, \ldots, p).$$

---

[1] Une propriété connue du déterminant adjoint montre même que chacun de ces mineurs est égal, au signe près, au déterminant du mineur de S^{-1} obtenu en conservant les m dernières colonnes et en supprimant les p lignes de même rang que les colonnes conservées de P; il est donc égal au quotient par $|\Delta(B)|$ du déterminant du mineur correspondant de A.

en posant

$$P = \left\| \begin{matrix} x_1^1 & x_1^2 & \dots & x_1^n \\ x_2^1 & x_2^2 & \dots & x_2^n \\ \dots & \dots & \dots & \dots \\ x_m^1 & x_m^2 & \dots & x_m^n \end{matrix} \right\|.$$

Les points de $\mathcal{C}$ contenus dans ce sous-espace forment un module $\mathcal{C}_m$ de dimension m : pour en obtenir une base, on peut suivre la marche indiquée précédemment : par un choix convenable des équations adjointes [1] on peut obtenir *comme base la matrice* N *qui a pour lignes les m dernières colonnes de* S^{-1}. On peut aussi vérifier ce résultat *a posteriori;* chacune des lignes de N vérifie bien les équations (7), ce qui résulte de $SS^{-1} = [1]$; donc N est un tableau de $\mathcal{C}_m$ et toute base est de la forme $\Sigma^{-1}N$, Σ à termes entiers; mais $|\Delta(\Sigma)|$ devant diviser les déterminants de tous les mineurs d'ordre m de N est égal à 1 et N est une base.

Les modules $\mathcal{C}_p$ et $\mathcal{C}_m$ constitués respectivement par toutes les solutions entières de systèmes de m et p équations, peuvent s'appeler *des modules de zéros rectangulaires* [2]. Pour se donner deux tels modules, on peut définir le sous-espace qui contient $\mathcal{C}_p$ par m équations linéaires indépendantes, à coefficients entiers, et alors le sous-espace de $\mathcal{C}_m$ est défini par m points entiers (coefficients des équations) et inversement. Il est à remarquer que si le plus grand commun diviseur de la matrice formée par les m points est 1, cette matrice est une base de $\mathcal{C}_m$; il suffit pour le prouver de faire un raisonnement analogue à celui qui a été fait pour la base N. Il est alors évident que tout module de points entiers de dimension inférieure à n est un module de zéros si le plus grand

---

(1) On peut prendre pour coefficients des équations adjointes les termes des autres lignes de S; on constitue ainsi un tableau B_1 dont les colonnes sont identiques aux lignes de S, en rangeant par exemple ces lignes dans l'ordre n, $n-1$, ..., 1, afin que les coefficients des équations (7) constituent les p dernières colonnes. Mais B_1 étant modulaire sa forme réduite est [1], et, pour l'y ramener, il faut le multiplier par B_1^{-1} dont les lignes sont identiques aux colonnes de S^{-1} prises en ordre inverse. La base de $\mathcal{C}_m$ s'obtient en prenant les m premières lignes de B_1^{-1}, donc les m dernières colonnes de S^{-1}.

(2) Dans l'espace à trois dimensions, l'un de ces modules est l'ensemble des points de $\mathcal{C}$ situés dans un plan passant par l'origine, l'autre est l'ensemble des points sur la droite issue de O et perpendiculaire au plan (en supposant les axes rectangulaires); d'où la dénomination précédente.

commun diviseur de sa base est 1 et un sous-module d'un module de zéros si ce plus grand commun diviseur est supérieur à 1.

Problèmes diophantiques.

On peut grouper, sous le nom d'*équations diophantiques* [1], les équations et systèmes d'équations dont on cherche la solution en nombres entiers. Nous nous occuperons seulement ici des systèmes d'équations linéaires à coefficients entiers. On peut ramener à ce cas celui des systèmes d'équations et congruences linéaires ; en effet, on peut toujours remplacer la résolution de l'équation congruentielle à n inconnues

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{a}$$

par celle de l'équation à $n+1$ inconnues

$$f(x_1, x_2, \ldots, x_n) - ay = 0.$$

Avant d'aborder le cas général, nous allons appliquer les méthodes et résultats précédents au cas bien connu d'une équation linéaire à deux inconnues, ou, ce qui est équivalent, d'une congruence linéaire à une inconnue

$$ax + by = c$$

ou

$$ax \equiv c \pmod{b}.$$

Les valeurs de la forme $\xi = ax + by$ pour x et y entiers forment un module de nombres dont la base est le plus grand commun diviseur d de a et b. D'ailleurs, en ajoutant à ξ la forme $\eta = x$, on obtient sans difficulté la base réduite du module de points (η, ξ)

$$\begin{Vmatrix} \frac{b}{d} & 0 \\ x_1 & d \end{Vmatrix} = \begin{Vmatrix} \frac{b}{d} & -\frac{a}{d} \\ x_1 & y_1 \end{Vmatrix} \times \begin{Vmatrix} 1 & a \\ 0 & b \end{Vmatrix};$$

---

[1] Cette dénomination n'est peut-être pas d'une très grande justesse historique. Il semble bien que Diophante est le premier des géomètres grecs qui se soit occupé des équations indépendamment de leur origine ou signification géométrique; mais il ne semble pas avoir toujours fait une distinction bien nette entre la recherche des solutions entières et celle des solutions quelconques.

donc, en appliquant les résultats établis dans le cas général,

$$ax + by = \lambda d,$$

$$(x, y) = (\mu, \lambda) \begin{Vmatrix} \frac{b}{d} & -\frac{a}{d} \\ x_1 & y_1 \end{Vmatrix}.$$

Pour que l'équation ait des solutions, il faut que c soit de la forme λd, c'est-à-dire soit divisible par le plus grand commun diviseur de a et b; s'il en est ainsi, les solutions sont données par

$$x = x_1 \frac{c}{d} - \mu \frac{b}{d}, \qquad y = y_1 \frac{c}{d} - \mu \frac{a}{d}.$$

Dans le cas de la congruence, les seules valeurs de x importent et pour avoir toutes les solutions distinctes (mod. b), il suffit de donner à μ, $d - 1$ valeurs incongrues (mod. d).

Passons à un système de m équations à n inconnues; nous supposerons qu'on a fait au préalable l'étude algébrique du système et que les équations considérées sont les *équations principales du système à résoudre*, *supposé possible ;* on a alors $m \leqq n$ et le rang de la matrice A des coefficients est m.

Si les équations sont homogènes, leurs solutions sont les points d'un module de zéros; elles s'expriment au moyen de $n - m$ indéterminées entières (il est alors nécessaire que n soit plus grand que m) et d'une matrice dont nous avons indiqué une détermination pratique ([1]). Les lignes d'une base P constituent un système de solutions particulières, qui est appelé par divers auteurs *système de solutions fondamentales*. Il y a une infinité de tels systèmes obtenus en remplaçant P par ΣP (Σ unimodulaire).

Les mêmes calculs sont encore applicables pour *m équations non homogènes*

(8) $$\xi_1 = u_1, \quad \xi_2 = u_2, \quad \ldots, \quad \xi_m = u_m;$$

pour qu'elles aient des solutions, il faut et il suffit que $(u_1, u_2, \ldots, u_m)$ soit un point du module $\mathfrak{M}$ formé par les points $(\xi_1, \xi_2, \ldots, \xi_m)$.

([1]) La méthode de résolution ainsi donnée par adjonction de $n - m$ colonnes complémentaires et réduction du tableau ainsi obtenu n'est pas, en somme, différente de celle indiquée par Euler (œuvres posthumes), signalée ensuite par Jacobi et reprise définitivement par Hermite (*cf.* STIELTJES, *loc. cit.*).

La vérification en est facile si l'on a mis la base de ce module sous la forme réduite B : il suffit de résoudre de proche en proche le système d'équations en λ_i,

$$\begin{aligned} u_m &= \lambda_m c_m^m, \\ u_{m-1} &= \lambda_m c_m^{m-1} + \lambda_{m-1} c_{m-1}^{m-1}, \\ &\dots\dots\dots\dots\dots\dots \\ u_1 &= \lambda_m c_m^1 + \lambda_{m-1} c_{m-1}^1 + \dots + \lambda_1 c_1^1 \end{aligned}$$

et de vérifier si les λ obtenus sont des entiers. S'il en est ainsi, les équations ont des solutions en nombres entiers données par la formule

$$\| x_1 \quad x_2 \quad \dots \quad x_n \| = \| \mu_1 \quad \dots \quad \mu_p \quad \lambda_1 \quad \dots \quad \lambda_m \| \times \mathrm{S},$$

les μ étant des indéterminées entières. En appelant P′ la matrice formée par les m dernières lignes de S,

$$\| x_1 \quad \dots \quad x_n \| = \| \mu_1 \quad \dots \quad \mu_p \| \times \mathrm{P} + \| \lambda_1 \quad \dots \quad \lambda_m \| \times \mathrm{P}'.$$

La première partie du deuxième membre est la solution générale des équations sans deuxième membre $\xi_i = 0$, la deuxième partie est une solution particulière des équations proposées, c'est une expression des solutions, dont les analogues sont bien connues (*voir* Chap. I, p. 14-15). On voit aussi qu'une partie des calculs peut encore servir si l'on change les deuxièmes membres.

On peut estimer que la condition ainsi trouvée pour la possibilité de solutions en nombres entiers n'est pas suffisamment symétrique ou élégante. Une autre condition a été indiquée par MM. Heger et Smith : *pour que les équations* (8) *aient des solutions en nombres entiers, il faut et il suffit que le plus grand commun diviseur de la matrice des coefficients des* ξ *soit identique au plus grand commun diviseur de cette même matrice complétée par une ligne formée des deuxièmes membres* [1].

---

[1] Cette condition d'un énoncé en apparence plus simple que le précédent peut être en réalité plus difficile à vérifier; il faut, en effet, former les déterminants des mineurs qui peuvent être en assez grand nombre et d'ordre assez élevé. Dans le cas de $m = n$, elle est identique à la résolution de l'équation par les formules de Cramer et à la vérification *a posteriori* que les solutions trouvées sont entières.

Le premier de ces plus grands communs diviseurs d est évidemment un multiple du second d'. Pour démontrer la réciproque, considérons les m équations homogènes à $n+1$ inconnues

$$\chi_1 = 0, \quad \ldots, \quad \chi_m = a_1 x_1 \ldots = a_n x_n - v x_0,$$

et cherchons la condition pour qu'elles aient un système de solutions entières où x_0 soit égal à 1. On peut prendre pour base du module de zéros des χ la matrice de type $(m+1, n+1)$

$$P_1 = \left\| \begin{matrix} & P & & & 0 \\ & & & & \vdots \\ & & & & 0 \\ v_1 & v_2 & \ldots & v_n & v_0 \end{matrix} \right\|;$$

alors il faut et il suffit que $v_0 = 1$. Or, on peut exprimer de diverses façons le déterminant d'un mineur de cette matrice contenant la dernière colonne. D'une part, il est égal à v_0 multiplié par le déterminant d'un mineur de P, c'est-à-dire d'un mineur de S (p premières lignes, colonnes de rang $i_1, \ldots, i_p$). Mais, d'après une propriété connue du déterminant adjoint, ce déterminant est égal au mineur de S^{-1} obtenu en supprimant les p premières colonnes et les lignes $i_1, \ldots, i_p$; nous avons vu que ce déterminant est lui-même égal au mineur correspondant de A (suppression des lignes $i_1, \ldots, i_p$), divisé par $|\Delta(B)| = d$. D'autre part, en raisonnant de même sur la matrice P_1, on trouve que le déterminant considéré est encore égal au quotient par d' du mineur de la matrice des coefficients des χ, obtenu par suppression des lignes de rang $i_1, \ldots, i_p$, et n, c'est-à-dire, en définitif, du mineur de A déjà trouvé. Donc $\frac{v_0}{d} = \frac{1}{d'}$ et la propriété est démontrée (1).

On peut encore ranger parmi les problèmes diophantiques la recherche des tableaux à termes entiers vérifiant certaines conditions. Nous nous contenterons d'indiquer ici deux problèmes posés

(1) On peut notamment appliquer ce résultat à l'étude du système de congruences $x_i \equiv \alpha_i \pmod{a_i}$ qu'on rencontre dans l'étude d'une congruence de module composé. La condition de possibilité est que chaque différence $|\alpha_i - \alpha_j|$ soit respectivement divisible par le plus grand commun diviseur de α_i, α_j. Comparer aussi cette démonstration avec la note (1), page 53.

et résolus par Hermite et dont la théorie précédente fournit également la solution.

I. *Étant donnée une matrice* M *à termes entiers de type* (m, n) *et de rang* m, *trouver une matrice* X *à termes entiers de type* $(n-m, n)$ *et de rang* $n-m$ *qui forme avec la première un déterminant ayant une valeur donnée, multiple toutefois du plus grand commun diviseur de* M. On peut traduire ce problème par l'équation symbolique

$$\Delta\begin{pmatrix} M \\ X \end{pmatrix} = k \times (\text{p. g. c. d. de M}).$$

M définit un sous-espace de dimension m et l'ensemble des points de $\mathcal{E}$ qui y sont contenus forme un module dont on sait déterminer une base M_1 (*voir* module rectangulaire); on a

$$M = T \times M_1, \qquad \Delta(T) = \text{p. g. c. d. de M}.$$

Les lignes de M_1 sont les m dernières colonnes d'un tableau unimodulaire S^{-1}; les $n-m$ premières colonnes prises comme lignes forment une matrice N_1 qui, avec la précédente, constitue un tableau unimodulaire

$$\begin{pmatrix} M_1 \\ N_1 \end{pmatrix}, \qquad \Delta\begin{pmatrix} M_1 \\ N_1 \end{pmatrix} = \pm 1.$$

Il est facile de déduire de là les solutions du problème proposé. D'une part, tout tableau $\begin{pmatrix} M \\ X \end{pmatrix}$ doit être égal au produit à droite du tableau modulaire $\begin{pmatrix} M_1 \\ N_1 \end{pmatrix}$ par un tableau à termes entiers Σ. Mais le produit par $\begin{pmatrix} M_1 \\ N_1 \end{pmatrix}$ de la matrice formée par les m premières lignes de Σ doit donner M. Cette matrice se compose donc du tableau T bordé de $n-m$ colonnes de zéros. On peut alors décomposer la matrice des $n-m$ dernières lignes de Σ en une matrice A formée par les m premières colonnes et un tableau Z formé par les $n-m$ dernières colonnes, soit d'une façon symbolique

$$\Sigma = \begin{pmatrix} T & 0 \\ A & Z \end{pmatrix}, \qquad \begin{pmatrix} M \\ X \end{pmatrix} = \Sigma \times \begin{pmatrix} M_1 \\ N_1 \end{pmatrix},$$

mais alors

$$k = (\text{p. g. c. d. M}) = |\Delta(\Sigma)| = |\Delta(T)| \times |\Delta(Z)|,$$
$$k = |\Delta(Z)|.$$

on a ainsi une restriction pour le tableau Z, mais c'est la seule et *Λ étant une matrice quelconque à termes entiers de type $(n-m, m)$ et Z un tableau à termes entiers d'ordre $n-m$, tel que $|\Delta(Z)| = k$, tout tableau*

$$\begin{pmatrix} T & 0 \\ \Lambda & Z \end{pmatrix} \times \begin{pmatrix} M_1 \\ N_1 \end{pmatrix} = \begin{pmatrix} T \times M_1 \\ X \end{pmatrix}$$

répond à la question et toutes les solutions du problème sont données par la formule

$$X = \Lambda M_1 + Z N_1.$$

On peut énoncer ainsi le second problème :

II. *Trouver une matrice de type $(n-1, n)$ telle que les déterminants de ses mineurs aient des valeurs données.* Si a_1, a_2, ..., a_n sont ces valeurs et si x_1, x_2, ..., x_n est une ligne quelconque de la matrice cherchée, on doit avoir

$$a_1 x_1 + \ldots + a_n x_n = 0,$$

donc chacune de ces matrices étant constituée par $n-1$ points du module de zéros $\mathcal{E}_{n-1}$ défini par cette équation, est une matrice de $\mathcal{E}_{n-1}$. Si M_1 est une base de $\mathcal{E}_{n-1}$, base qu'on sait pratiquement trouver, les déterminants des mineurs de M_1 sont

$$\frac{a_1}{d}, \quad \frac{a_2}{d}, \quad \ldots, \quad \frac{a_n}{d}, \qquad d = (a_1, a_2, \ldots, a_n).$$

Toute matrice de $\mathcal{E}_{n-1}$ est de la forme ΣM_1 (Σ à termes entiers) et les déterminants de ses mineurs sont $\Delta(\Sigma) \times \frac{a_i}{d}$. *Toutes les solutions du problème sont donc données par la formule*

$$\Sigma \times M_1,$$

Σ étant un tableau à termes entiers quelconques, mais dont le déterminant est égal à d.



CHAPITRE IV.

LES NOMBRES ET LES ENTIERS ALGÉBRIQUES.

Nous allons, dans ces deux Chapitres, appliquer les considérations précédentes aux *nombres algébriques*. On appelle ainsi les racines réelles ou imaginaires d'équations algébriques à coefficients rationnels ou entiers. Bien entendu, nous ne soulèverons ici aucune difficulté au sujet de l'existence de ces racines et supposerons acquis le théorème de d'Alembert [1]. Ces nombres sont, en somme, les plus simples après les nombres rationnels et il semble naturel d'attacher une assez grande importance à leur étude. Ce fut d'ailleurs une des préoccupations essentielles d'Hermite qui voyait dans la recherche des propriétés particulières ou caractéristiques des nombres algébriques un des problèmes les plus importants de la Théorie des Nombres [2]. A l'heure actuelle ce problème est loin d'être résolu ; mais une partie de la question a donné lieu, surtout en Allemagne, à des développements importants; c'est l'extension à certains ensembles de nombres algé-

(1) Toute démonstration de ce théorème, qui est vrai pour des coefficients quelconques, repose en général sur l'idée de continuité, c'est-à-dire sur une définition du nombre irrationnel général, par exemple, au moyen d'une coupure. On pourrait chercher à montrer l'existence logique des nombres algébriques et de leur calcul à partir de la seule idée de nombre entier. C'est ce qu'a fait M. J. Drach dans TANNERY, *Introduction à l'étude de la Théorie des Nombres*, Paris, 1895.

(2) « Dans cette immense étendue de recherches qui nous a été laissée par M. Gauss », écrit-il à Jacobi, « l'Algèbre et la Théorie des Nombres me paraissent devoir se confondre dans un même ordre de notions analytiques dont nos connaissances actuelles ne nous permettent pas encore de nous faire une juste idée. Peut-être cependant doit-on entrevoir qu'il appartiendra à cette partie de la Science, constituée ainsi sur ses véritables bases, d'offrir le tableau de tous les éléments, en nombre fini ou illimité, dont dépendent les racines des équations algébriques, séparés en types irréductibles et classés suivant leurs rapports naturels. »

briques des propriétés des nombres rationnels et des nombres entiers. C'est surtout de cette extension que nous nous occuperons ici.

Polynomes et équations.

Rappelons d'abord quelques notions élémentaires sur les polynomes et les équations algébriques : nous avons cité le théorème de d'Alembert, il entraine l'existence de n racines pour une équation algébrique de degré n et l'on sait que les fonctions symétriques rationnelles de ces racines s'expriment rationnellement au moyen des coefficients. Les racines communes à deux équations, ou les racines d'un ordre de multiplicité déterminé d'une équation sont les zéros simples d'un polynome qu'on peut former par des opérations rationnelles à partir des polynomes premiers membres des équations données.

Ces propriétés qui sont vraies, quels que soient les coefficients, montrent l'importance de la notion de domaine de rationalité. On appelle *domaine de rationalité de* $\alpha_1, \alpha_2, \ldots, \alpha_k$ l'ensemble des fonctions rationnelles à coefficients rationnels de $\alpha_1, \alpha_2, \ldots, \alpha_k$; ceci peut l'étendre au cas où les α seraient en nombre infini. Si les coefficients d'une équation sont numériques, ce que nous supposerons toujours, le domaine de rationalité qu'ils définissent est un ensemble de nombres; on voit immédiatement comment, avec cette locution, on peut énoncer les principes rappelés.

Mais on peut aussi envisager un domaine de rationalité R, numérique, défini *a priori*, et les polynomes dont les coefficients sont dans ce domaine, on dit, pour abréger, les *polynomes de* R. On dit alors qu'un polynome de R est *irréductible dans* R s'il n'est divisible par aucun autre polynome [1] de R. Les polynomes irréductibles jouent en quelque sorte le rôle de facteurs premiers dans le domaine; tout polynome qui n'est pas irréductible est décomposable d'une seule façon en un produit de facteurs irréductibles, en ne distinguant pas un diviseur et son

---

[1] Dans le cas où le domaine est l'ensemble de tous les nombres réels ou imaginaires, les seuls polynomes irréductibles sont tous les binomes du premier degré; dans le cas de l'ensemble des nombres réels, il faut ajouter à ces binomes les trinomes du second degré, somme de deux carrés.

produit par un facteur numérique; le plus grand commun diviseur d'un polynome $G(x)$ et d'un autre $F(x)$ irréductible dans le même domaine R, ne peut être que F lui-même ou une constante numérique. En rapprochant ceci des relations évidentes entre la divisibilité et les zéros, on obtient ce principe d'une application constante.

Si un polynome $G(x)$ *de* R *admet un zéro d'un polynome* $F(x)$ *irréductible dans* R, $G(x)$ *est divisible par* $F(x)$ *et, par suite, admet tous les zéros de* F [1].

En effet, le zéro commun doit annuler le plus grand commun diviseur de F et G, qui, étant ainsi de degré non nul, ne peut être que F.

Plaçons-nous maintenant dans le cas du domaine des nombres rationnels. Si l'on s'occupe surtout des équations et de leurs racines, on peut toujours supposer que, après réduction des termes semblables, *les coefficients des polynomes premiers membres sont des nombres entiers premiers entre eux;* d'après une dénomination de Gauss *un tel polynome est dit primaire.* L'introduction de ces polynomes est justifiée par la propriété due aussi à Gauss :

Le produit FG *de deux polynomes primaires est encore un polynome primaire.*

Nous allons montrer qu'il est impossible que les termes du produit soient divisibles par un nombre premier p; séparons dans $F(x)$ les termes, s'ils existent, dont les coefficients sont divisibles par p, soit $f(x)$ le polynome qu'ils forment

$$F(x) = f(x) + \varphi(x), \qquad \varphi(x) = \alpha_0 x^{\mu} + \alpha_1 x^{\mu-1} + \ldots$$

(les α non divisibles par p),

$f(x)$ peut être identiquement nul, mais d'après l'hypothèse $\varphi(x)$ existe et l'on peut supposer $\alpha_0 \neq 0$. De même, pour $G(x)$,

$$G(x) = g(x) + \gamma(x), \qquad \gamma(x) = \beta_0 x^{\nu} + \beta_1 x^{\nu-1} + \ldots.$$

---

[1] Dans les cours de Spéciales on démontre ce principe pour le domaine des nombres réels, c'est le théorème sur les racines imaginaires conjuguées.

Mais alors on a

$$F(x)G(x) - f(x)g(x) - f(x)\psi(x) - g(x)\varphi(x) = \varphi(x)\psi(x).$$

Si tous les coefficients de FG étaient divisibles par p, il en serait de même des coefficients du polynome premier membre de cette égalité, mais ceci est absurde, car dans le deuxième membre, le coefficient $\alpha_0\beta_0$ du terme de plus haut degré n'est pas divisible par p, α_0 et β_0 ne l'étant pas.

On peut donner des formes plus ou moins diverses à l'énoncé précédent : il en résulte notamment que : *si un polynome à coefficients entiers est divisible par un polynome primaire, le quotient a ses coefficients entiers.* Car, en mettant en facteur dans les termes de ce quotient leur plus grand commun diviseur, on peut le mettre sous la forme $\frac{a}{d}f(x)$, f étant primaire ; le polynome primitif est donc le produit de $\frac{a}{d}$ par un polynome primaire (produit de deux tels polynomes) ; donc $\frac{a}{d}$ est un entier, et c'est ce qu'il fallait démontrer. On peut encore en conclure que si *un polynome à coefficients entiers est décomposable en un produit de facteurs dans le domaine des nombres rationnels, on peut toujours supposer que ses facteurs sont à coefficients entiers.*

Remarquons en terminant que ces considérations s'étendent immédiatement à des polynomes à plusieurs variables $F(x, y, z)$. Il suffit de ranger leurs termes par hauteur, ou ce qui revient au même, de faire le changement de variables indiqué par Kronecker

$$x = t, \qquad y = t^{\omega}, \qquad z = t^{\omega^2},$$

ω étant choisi assez grand ; à chaque terme du polynome en t ainsi obtenu correspond un et un seul terme de l'ancien polynome en x, y, z, et réciproquement. Les coefficients sont donc les mêmes et l'on a les mêmes réductions dans le produit de deux polynomes en x, y, z, et dans le produit des polynomes en t correspondants.

Corps algébriques.

D'après ce qui précède, un nombre algébrique α est toujours racine d'une équation $F(x) = 0$, $F(x)$ étant primaire et irréductible dans le domaine des nombres rationnels ; ce polynome est en outre unique, au produit près par -1 : tout autre polynome

$F_1(x)$ ayant α pour zéro est un multiple de $F(x)$; s'il est irréductible il n'en peut différer que par un facteur numérique et ce facteur est ± 1, si F_1 comme F est primaire. *Le degré de* F, qui est ainsi bien déterminé, est dit *le degré du nombre algébrique* α *et les n racines de l'équation*, $\alpha_1, \alpha_2, \ldots, \alpha_n$, dont l'une est α, *les nombres conjugués de* α; d'après le théorème sur les équations irréductibles, toute relation rationnelle à coefficients rationnels vérifiée par un nombre algébrique est vérifiée par tous ses conjugués. Il est aussi commode, quoique moins usuel, de donner *un nom à* $F(x)$, par exemple, le *polynome* ou l'*équation fondamentale de* α. Les nombres rationnels sont des nombres algébriques de degré 1, donc sans conjugués.

Les fonctions symétriques rationnelles à coefficients rationnels des n nombres conjugués de α sont des nombres rationnels. Certaines d'entre elles ont reçu des dénominations d'un usage assez commode : *le produit* $\alpha_1\alpha_2\ldots\alpha_n$ est dit la *norme de* α : $N(\alpha)$; *la somme* $\alpha_1+\alpha_2+\ldots+\alpha_n$ est dite *la trace* (du mot allemand Spur); enfin *le produit des carrés des différences*

$$\Pi(\alpha_i-\alpha_j)^2=\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ (\alpha_1)^2 & (\alpha_2)^2 & \ldots & (\alpha_n)^2 \\ \ldots & \ldots & \ldots & \ldots \\ (\alpha_1)^{n-1} & (\alpha_2)^{n-1} & \ldots & (\alpha_n)^{n-1} \end{vmatrix}^2$$

est appelé *le discriminant* du nombre; c'est d'ailleurs, à un facteur numérique près, ce qu'on appelle habituellement le discriminant de l'équation fondamentale.

Ceci posé, envisageons plusieurs nombres algébriques en nombre fini α, β, γ et le domaine de rationalité qu'ils définissent. L'ensemble des nombres $K(\alpha, \beta, \gamma)$ ainsi obtenu est connu sous le nom *de corps algébrique* (¹). Tout nombre de K

$$\varpi=\varphi(\alpha, \beta, \gamma)$$

(¹) Cette notion de corps qui remonte à Galois peut s'étendre en partant d'un domaine de rationalité plus général que celui des nombres rationnels. Mais alors on fait une distinction assez nette entre les éléments du domaine de rationalité et les éléments nouveaux introduits qu'on se propose plus ou moins de calculer au moyen d'expressions algébriques plus simples. Au contraire, dans ce qui suit, nous ne nous attacherons pas à la recherche d'une expression particulière des nombres algébriques, mais plutôt à l'arithmétique de l'ensemble des nombres du corps.

est encore un nombre algébrique. On peut le voir en éliminant α, β, γ entre cette équation et les équations fondamentales de ces nombres ; ou, ce qui revient au même, en formant les fonctions symétriques élémentaires de tous les nombres obtenus en remplaçant dans ϖ de toutes les façons possibles α, β, γ par leurs conjugués. Ces fonctions étant séparément symétriques par rapport aux α_i, β_j, γ_k sont des nombres rationnels ; ce sont les coefficients d'une équation dont ϖ est racine ; le degré de cette équation est le produit des degrés de α, β, γ, mais comme elle n'est pas nécessairement irréductible, on peut seulement affirmer qu'on a ainsi un multiple du degré de ϖ. Il n'y a pas lieu d'attacher d'importance au nombre d'irrationnelles distinctes α, β, γ, car, ainsi que l'a montré Galois, *tout corps algébrique peut être engendré par un seul de ses éléments convenablement choisi.*

Considérons en effet une fonction rationnelle à coefficients rationnels de 3 variables (autant que d'irrationnelles qui servent à définir le corps)

$$\psi(x, y, z),$$

assujettie à prendre des valeurs distinctes quand on y remplace x, y, z respectivement par les nombres conjugués de α, β, γ de toutes les façons possibles ; on aura, par exemple, une telle fonction en considérant $ux + vy + wz$, u, v, w étant des fractions convenablement choisies [1]. La fonction ψ étant choisie, soit ω sa valeur pour α, β, γ, ce nombre ω est dans $K(\alpha, \beta, \gamma)$ et il en est de même de tout nombre de $K(\omega)$. Pour démontrer la réciproque, formons le produit

$$\Phi(\omega, x) = \prod_{j,l} [\omega - \psi(x, \beta_j, \gamma_l)],$$

étendu à tous les nombres conjugués de β et γ ; Φ, d'après une

---

(1) Pour montrer la possibilité de ce choix considérons toutes les différences possibles des valeurs de cette fonction prises deux à deux et séparons-les en trois groupes : celles qui ne contiennent ni u, ni v ; celles qui contenant v, ne contiennent pas u ; enfin celles qui contiennent u. Pour qu'aucune des différences du premier groupe ne soit nulle, il suffit de choisir w non nul ; ce choix fait, les valeurs de v qui annulent les différences du deuxième groupe sont en nombre fini, on peut donc choisir v rationnel et différent des valeurs précédentes ; de même, pour le choix de u, et ainsi de suite s'il y a plus de trois irrationnelles.

remarque précédente, est une fonction rationnelle en ω et x, à coefficients rationnels. Son numérateur $F(x)$, considéré comme polynome en x, appartient au domaine $K(\omega)$, il ne s'annule pour aucun des nombres conjugués de α, à l'exception de α lui-même, puisque d'après l'hypothèse aucun des facteurs du second membre n'est nul. Mais alors si $f(x) = 0$ est l'équation fondamentale de α, le plus grand commun diviseur de F et f a α pour seul zéro, il est donc du premier degré et α est le quotient de ses coefficients. Or, $f(x)$ étant à coefficients rationnels appartient *a fortiori* à $K(\omega)$, il en est de même du plus grand commun diviseur et par suite de α. On le vérifierait de même pour β et γ et il en est par conséquent ainsi pour tout nombre de $K(\alpha, \beta, \gamma)$; la démonstration est évidemment générale.

Tout nombre qui peut ainsi engendrer un corps algébrique est dit un élément primitif du corps. Si ω et ω' sont deux éléments primitifs d'un même corps, ω appartient à $K(\omega')$ et a un degré au plus égal à celui de ω'; de même pour ω' par rapport à ω, il en résulte que *les degrés de deux et, par suite, de tous les éléments primitifs du corps sont égaux, ce degré commun est dit le degré du corps*. D'autre part, la démonstration précédente appliquée à $K(\omega)$ montre que pour engendrer ce corps on peut remplacer ω par toute fonction rationnelle à coefficients rationnels

$$\omega' = \theta(\omega),$$

pourvu que $\theta(x)$ prenne n valeurs distinctes, quand on remplace x par les n nombres conjugués de ω. On obtient ainsi de nouveaux éléments primitifs à partir de l'un d'entre eux; c'est la seule façon d'en obtenir. En effet, si les n valeurs $h(\omega_i)$ d'une fonction $h(x)$ ne sont pas distinctes, ces n valeurs sont racines d'une équation à coefficients rationnels de degré n mais à racines multiples; donc, l'élément du corps $h(\omega)$, racine particulière de cette équation, est de degré inférieur à n et ne saurait être un élément primitif. On voit en outre que tout élément imprimitif est de degré inférieur à celui du corps, ce qui permet de définir *les éléments primitifs comme ceux de degré maximum*.

Si dans les fonctions qui constituent $K(\omega)$, *on remplace* ω *par ses n conjugués, on obtient n corps*, $K(\omega_1)$, $K(\omega_2)$, ..., $K(\omega_n)$,

dits corps conjugués de K. Aux valeurs ω_i réelles correspondent des corps réels formés d'éléments réels et à des couples de valeurs imaginaires conjuguées des corps imaginaires conjugués : on peut donc distinguer pour un corps donné, outre le degré n le nombre r de corps réels et le nombre $2s$ de corps imaginaires conjugués deux à deux ($r+2s=n$). Les nombres de ces corps se correspondent de façon biunivoque et à la somme ou au produit correspond la somme ou le produit; en outre toute relation à coefficients rationnels entre certains éléments d'un corps existe aussi entre les éléments correspondants de chacun des autres (puisqu'elle est, toute réduction faite, une relation en ω et par suite vérifiée par tous les conjugués de ω). Si l'on considère un élément primitif $\omega' = \theta(\omega)$, il lui correspond dans les n corps des éléments distincts $\omega'_i = \theta(\omega_i)$ qui vérifient l'équation fondamentale de ω'; ce sont par conséquent les conjugués de ω', et chacun d'eux est primitif dans le corps auquel il appartient. Donc, de même que pour le degré, la définition et la correspondance des corps conjugués est indépendante de l'élément primitif dont on se sert pour engendrer K.

Que se passe-t-il pour un élément imprimitif $\varpi = h(\omega)$? Les n nombres $\varpi_i = h(\omega_i)$ ne sont plus distincts et le polynome

$$F(x) = (x-\varpi_1)(x-\varpi_2)\dots(x-\varpi_n)$$

a des zéros multiples et par suite des diviseurs à coefficients rationnels. Mais si $f(x) = 0$ est l'équation fondamentale de ϖ, elle est vérifiée par $\varpi_1, \varpi_2, \dots, \varpi_n$; $F(x)$ qui est divisible par $f(x)$ ne peut donc avoir de facteur distinct de celui-là et en est une puissance exacte $F(x) = [f(x)]^k$. Par conséquent, les nombres ϖ_i se répartissent en $\frac{n}{k}$ groupes de k nombres respectivement égaux aux racines d'une équation irréductible de degré $\frac{n}{k}$; par extension, $\varpi_1, \varpi_2, \dots, \varpi_n$ sont encore appelés *les conjugués de* ϖ. Il y a donc lieu de distinguer les conjugués d'un nombre algébrique au point de vue absolu, ou considéré comme appartenant à un corps donné : ces deux notions ne se confondent que si le nombre est primitif dans le corps. On fait la même distinction pour sa norme et sa trace. En particulier, les conjugués d'un nombre rationnel considéré

comme appartenant à un corps de degré n sont n nombres égaux [1] à $\frac{p}{q}$ et sa norme et sa trace sont $\left(\frac{p}{q}\right)^n$ et $n\frac{p}{q}$. Remarquons enfin que le degré d'un élément imprimitif est un diviseur de n, et qu'il n'y a pas de tels éléments [2] (à l'exception des nombres rationnels), si n est premier.

Représentation des nombres d'un corps.

Nous avons ainsi montré la possibilité de la réalisation pratique d'une arithmétique d'un corps algébrique K; chaque opération dans K se ramène à un calcul sur un élément primitif choisi, et la constatation de l'égalité de deux éléments à la divisibilité d'un polynome par le polynome fondamental $F(x)$ de l'élément primitif. Pour éviter cette dernière recherche il peut être commode d'avoir une représentation unique de chaque élément du corps au moyen de l'élément primitif. D'autre part, comme l'arithmétique de K est identique à celle de ses conjugués, il est naturel de chercher une représentation unique des termes des n corps, pour laquelle il ne soit pas nécessaire de faire à l'avance une séparation des racines de l'équation $F(x) = 0$.

Le premier de ces desiderata est rempli par le principe suivant :

Si ω *est un élément primitif du corps, tout élément* ϖ *de* $K(\omega)$ *peut être mis sous la forme*

$$(1) \qquad \varpi = a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{n-1}\omega^{n-1} \qquad (a_i \text{ rationnels}),$$

et ceci d'une seule façon.

Soit en effet $F(x) = 0$ l'équation caractéristique de ω et considérons un élément du corps

$$\varpi = \frac{f(\omega)}{g(\omega)},$$

---

[1] On peut rapprocher ceci de la définition d'un système simple [m], pour laquelle il est nécessaire de connaître l'ordre du tableau. On verra ci-après que ce rapprochement n'est pas tout à fait fortuit.

[2] La recherche des éléments imprimitifs est surtout utile pour la résolution de l'équation. Toutes les notions précédentes s'étendent d'ailleurs immédiatement au cas d'un domaine de rationalité quelconque.

$f(x)$ et $g(x)$ étant des polynomes à coefficients entiers premiers entre eux (sinon on pourrait les diviser par leur plus grand commun diviseur à termes entiers), $g(x)$ et $F(x)$ sont aussi premiers entre eux, sinon F diviserait g et $g(\omega)$ serait nul, $f(\omega)$ ne l'étant pas. Donc, par application du théorème de Bezout, on peut trouver $P(x)$ et $Q(x)$ à coefficients rationnels tels que

$$P(x)g(x) + Q(x)F(x) = 1.$$

en remplaçant dans cette identité x par ω, on obtient

$$P(\omega)g(\omega) = 1, \qquad \varpi = f(\omega)P(\omega) = f_1(\omega).$$

On a ainsi mis ϖ sous la forme d'un polynome en ω, mais d'après l'identité de la division, $f(x)$ et le reste $R(x)$ de sa division par $F(x)$ prennent la même valeur pour ω. Donc $\varpi = R(\omega)$ et, comme R est au plus de degré $n-1$, on a bien une égalité [1] de la forme (1). Une telle représentation est en outre unique, car si deux polynomes de degré inférieur à n, $R(x)$ et $R'(x)$ prennent la même valeur pour ω, leur différence, de degré inférieur à n, est identiquement nulle ou divisible par $F(x)$, et ce dernier cas est impossible. Cette démonstration fournit en même temps une méthode de calcul des éléments de $K(\omega)$; il suffit de faire le calcul sur les polynomes (1), en considérant ω comme variable, et en remplaçant à la fin ou dans le cours du calcul, toute fraction par un polynome (1) au moyen du procédé ci-dessus.

Ceci établi, si nous envisageons simultanément les n conjugués

$$\varpi_1, \varpi_2, \ldots, \varpi_n$$

d'un terme de K, on peut considérer qu'ils représentent un point d'un espace à n dimensions, peut être semi-réel; on obtient ainsi un module de points $\mathfrak{R}$. Mais, d'après ce qui précède, *on peut trouver un tableau Ω du module tel que tout point de $\mathfrak{R}$ ait par rapport à Ω des coordonnées rationnelles et réciproquement.* En effet, en ayant égard à ce que l'égalité (1) subsiste si l'on

---

(1) Cette méthode est en somme une extension très naturelle de l'exposé donné habituellement du calcul des imaginaires (point de vue des équivalences de CAUCHY). C'est x^2+1 qui joue le rôle de $F(x)$; toutefois, dans le calcul des imaginaires on ne suppose pas les coefficients des fonctions rationnels; si on le faisait, on aurait l'arithmétique du corps $K(i)$.

remplace ϖ et ω par leurs conjugués, et sans changer les a, on peut l'écrire

$$\varpi_1\ \ \varpi_2\ \ \dots\ \ \varpi_n = a_0\ \ a_1\ \ \dots\ \ a_{n-1} \times \Omega,$$

$$\Omega = \left\| \begin{matrix} 1 & 1 & \dots & 1 \\ \omega_1 & \omega_2 & \dots & \omega_n \\ (\omega_1)^2 & (\omega_2)^2 & \dots & (\omega_n)^2 \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ (\omega_1)^{n-1} & (\omega_2)^{n-1} & \dots & (\omega_n)^{n-1} \end{matrix} \right\|$$

et réciproquement, si les a sont rationnels, ϖ est un nombre du corps. On peut, sans changer cette propriété, remplacer Ω par tout tableau $\Pi = R\Omega$, R à termes rationnels et à déterminant différent de o; ce tableau Π ainsi obtenu est constitué par n points de $\mathcal{R}$; on peut même choisir arbitrairement ces n points pourvu toutefois que le déterminant de leur tableau ne soit pas nul. *Un tel tableau* Π *sera dit une base du corps.* Le nombre r de colonnes réelles de cette base est égal au nombre des corps conjugués de K qui sont réels; et de même pour $2s$, il est en effet impossible qu'une colonne correspondant à un corps imaginaire soit entièrement formée de termes réels, sinon la colonne correspondant au corps imaginaire conjugué serait identique à la précédente et $\Delta(\Pi)$ serait nul.

Mais si cette représentation géométrique est bonne quand il s'agit de la somme des nombres du corps (et nous nous en servirons ultérieurement dans ce but), elle ne l'est plus pour le produit, cette opération n'étant pas invariante pour un changement de coordonnées. On a une représentation plus appropriée en faisant correspondre à tout nombre ϖ du corps le tableau canonique

$$[\varpi_1, \varpi_2, \dots, \varpi_n],$$

ou tout tableau

$$X = P[\varpi_1, \varpi_2, \dots, \varpi_n]P^{-1}, \qquad \Delta(P) \neq 0.$$

A toute fonction rationnelle de plusieurs nombres du corps ou de leurs conjugués correspond la même fonction rationnelle des tableaux X correspondants (*voir* les ensembles abéliens de tableaux, premier Chapitre). L'intérêt de cette représentation est qu'on peut choisir P de façon que tous les tableaux X aient leurs termes rationnels; il suffit de prendre pour P une des bases Π

du corps. En effet, si $\alpha, \beta, \ldots, \lambda$ sont les nombres qui constituent H, les nombres $\alpha\varpi, \beta\varpi, \ldots, \lambda\varpi$ appartiennent au corps, d'où les n égalités, les $a, b, \ldots, l$ étant des nombres rationnels,

$$\begin{aligned} \|\alpha_1\varpi_1 \quad \alpha_2\varpi_2 \quad \ldots \quad \alpha_n\varpi_n\| &= \|a_1 \quad \ldots \quad a_n\| H, \\ \|\beta_1\varpi_1 \quad \beta_2\varpi_2 \quad \ldots \quad \beta_n\varpi_n\| &= \|b_1 \quad \ldots \quad b_n\| H, \\ \ldots \quad \ldots \quad \ldots \quad \ldots & \quad \ldots \quad \ldots \\ \|\lambda_1\varpi_1 \quad \lambda_2\varpi_2 \quad \ldots \quad \lambda_n\varpi_n\| &= \|l_1 \quad \ldots \quad l_n\| H, \end{aligned}$$

qui sont équivalentes à l'égalité entre tableaux [1]

$$(2) \qquad H[\varpi_1, \varpi_2, \ldots, \varpi_n] H^{-1} = \begin{Vmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \\ \ldots & \ldots & \ldots & \ldots \\ l_1 & l_2 & \ldots & l_n \end{Vmatrix}.$$

Les lignes du tableau sont les coordonnées relatives par rapport à H des points de $\mathfrak{R}$ correspondant à $\alpha\varpi, \beta\varpi, \ldots, \lambda\varpi$.

L'opérateur commun des tableaux étant ainsi choisi égal, à une dilatation près, à l'une des bases du corps K(ω), tous les tableaux à termes rationnels correspondant aux nombres de K forment *un ensemble abélien* (où la multiplication est commutative); cet ensemble n'est pas extensible, c'est-à-dire que *tout tableau* Y *à termes rationnels permutable avec les tableaux de l'ensemble appartient aussi à l'ensemble et correspond à un seul nombre du corps*. En effet, si X_1 est un tableau correspondant à un élément primitif, l'équation en λ de X_1 n'a pas de racines doubles et Y permutable avec X_1 a même opérateur, soit H. D'autre part, toute racine de l'équation en λ de Y s'exprime rationnellement au moyen des termes de Y qui sont rationnels et des termes d'une colonne déterminée de H; donc cette racine appartient à un des corps conjugués de K et Y est de la forme (2), son tableau canonique étant formé par les coordonnées d'un point de $\mathfrak{R}$.

La norme d'un nombre de K *est égal au déterminant du tableau correspondant, la trace à la somme des termes de la diagonale principale;* enfin aux nombres rationnels $\frac{p}{q}$, qui appartiennent tous au corps, correspondent les systèmes simples $\left[\frac{p}{q}\right]$ qui appartiennent tous à l'ensemble des tableaux.

---

[1] Ce calcul n'est pas, en somme, différent de celui indiqué par Hermite pour la transformation de Tschirnhausen.

Ce qui précède fournit un moyen de constituer *a priori* un corps algébrique, ou plutôt un ensemble de tableaux qui lui corresponde. Il suffit de se donner un tableau X à termes rationnels dont on a pu vérifier que l'équation en λ était irréductible, ou encore de se donner cette équation $f(\lambda) = 0$ (ses zéros étant $\omega_1, \omega_2, \ldots, \omega_n$) et de chercher un tableau à termes rationnels qui l'admette pour équation [1] en λ. Alors, tous les tableaux à termes rationnels permutables avec X forment un ensemble dont les éléments correspondent univoquement aux nombres des n corps conjugués $K(\omega_i)$. Le tableau X peut, en effet, être mis sous la forme (2); l'ordre des ω_i étant arbitrairement choisi, l'opérateur de X est défini à une dilatation près, les rapports mutuels des termes de la $i^{\text{ème}}$ colonne sont des fonctions rationnelles à coefficients rationnels de ω_i, c'est-à-dire des nombres de $K(\omega_i)$, les rapports mutuels des termes dans les autres colonnes sont les nombres correspondants des corps conjugués de K; donc on peut, en disposant de la dilatation arbitraire, supposer que cet opérateur est une base de $K(\omega)$; on est alors ramené à la discussion précédente.

Entiers d'un corps.

Que l'on considère les nombres algébriques d'un corps ou leur représentation par des tableaux, on obtient un ensemble où sont possibles les quatre opérations élémentaires. On peut donc dire qu'il jouit des propriétés des nombres rationnels (il contient d'ailleurs tous ces nombres). Peut-on, parmi les nombres du corps, choisir des nombres particuliers dont l'ensemble $\mathcal{O}$ jouisse de propriétés analogues à celles de l'ensemble des entiers ordinaires? Il faut d'abord que toute fonction entière à coefficients entiers de plusieurs termes de $\mathcal{O}$ soit dans $\mathcal{O}$ (c'est là la définition ordinaire d'un domaine d'intégrité dans un domaine de rationalité); nous y ajouterons la condition que les termes de $\mathcal{O}$ se déduisent

---

[1] On verra aisément comment on peut constituer un tel tableau à partir de cette équation. On peut d'ailleurs exposer ce mode de représentation sans se servir de l'existence des racines en tant que nombres irrationnels complexes. On répondrait ainsi aux desiderata de M. Drach et l'on aurait une preuve plus tangible de l'existence logique des racines.

par addition et soustraction d'un nombre fini d'entre eux ([1]) (de même que les entiers ordinaires se déduisent de l'unité par addition et soustraction). Il est assez curieux, et c'est même l'un des points essentiels de cette théorie, que ces propriétés de l'ensemble $\mathfrak{O}$ conduisent à des conditions indépendantes du corps K pour les nombres qui constituent $\mathfrak{O}$.

La condition nécessaire et suffisante pour qu'un nombre algébrique du corps K *fasse partie d'un tel ensemble* $\mathfrak{O}$ *est qu'il soit racine d'une équation :*

$$(3) \qquad x^N + a_1 x^{N-1} + \ldots = 0 \qquad (a \text{ entiers}).$$

Toute racine d'une telle équation est dite, pour cette raison, entier complexe.

Soit d'abord un ensemble $\mathfrak{O}$ de nombres d'un corps et supposons qu'on puisse déduire chacun de ses termes par addition et soustraction de p d'entre eux, α, β, ..., λ. C'est dire que chaque élément de $\mathfrak{O}$ est une combinaison linéaire et homogène à coefficients entiers de α, β, ..., λ. Alors, si ϖ est un nombre de $\mathfrak{O}$, il en est de même de $\alpha\varpi$, $\beta\varpi$, ..., $\lambda\varpi$, et l'on doit avoir :

$$\begin{aligned} \varpi\alpha &= a_1^1\alpha + a_1^2\beta + \ldots + a_1^p\lambda, \\ \varpi\beta &= a_2^1\alpha + a_2^2\beta + \ldots + a_2^p\lambda, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varpi\lambda &= a_p^1\alpha + a_p^2\beta + \ldots + a_p^p\lambda, \end{aligned}$$

les a étant des entiers ordinaires. En considérant ces égalités comme des équations en α, β, ..., λ, on en déduit

$$\begin{vmatrix} a_1^1 - \varpi & a_1^2 & \ldots & a_1^p \\ a_2^1 & a_2^1 - \varpi & \ldots & a_2^p \\ \ldots & \ldots\ldots & \ldots & \ldots \\ a_p^1 & a_p^2 & \ldots & a_p^p - \varpi \end{vmatrix} = 0;$$

c'est dire que ϖ vérifie bien une équation ([2]) de la forme (3).

([1]) On vérifie sans peine que ces propriétés ne sont vérifiées dans le corps des nombres rationnels que par des ensembles formés d'entiers ordinaires (multiples d'un même nombre).

([2]) Il est à remarquer que, pour cette démonstration, on n'a pas utilisé l'hypothèse que les nombres sont algébriques. On prouve donc encore (ainsi que l'a établi M. Dedekind) qu'un ensemble de nombres, vérifiant les deux conditions imposées à $\mathfrak{O}$, est nécessairement formé de nombres algébriques.

Avant de démontrer la réciproque, indiquons quelques propriétés des entiers complexes ainsi définis. L'équation fondamentale $F(x) = 0$ d'un tel entier α est aussi de la forme (3), car, F étant primaire, d'après la propriété de Gauss, tout polynome à coefficients entiers $f(x)$ ayant α pour zéro est le produit de $F(x)$ par un polynome à coefficients entiers, donc le coefficient du terme de plus haut degré de F est un diviseur de celui de f; si ce dernier est égal à ± 1, il en est de même du premier. Ceci conduit à une autre définition des entiers complexes : *ce sont des nombres algébriques tels que les fonctions symétriques élémentaires et, par suite, toutes les fonctions symétriques entières à coefficients entiers de leurs conjugués* (*le nombre considéré en lui-même ou comme appartenant à un corps*) *sont des nombres entiers rationnels*. En particulier, les entiers complexes de degré 1 (ou rationnels) ne sont autres que les entiers ordinaires. Enfin, dans un corps, il existe bien une infinité d'entiers complexes et tout autre terme est le quotient d'un entier complexe par un entier ordinaire; en effet, si ϖ est un nombre de K et a_0 un dénominateur commun des fonctions symétriques élémentaires de ϖ, le nombre $a_0\varpi$ appartient à K et les fonctions symétriques élémentaires de ses conjugués sont des entiers. Si ϖ est primitif, l'entier $a_0\varpi$ est également primitif.

Ceci acquis, pour démontrer que la condition est suffisante, nous allons établir que tous les entiers complexes d'un corps K forment bien un ensemble $\mathcal{O}$ répondant aux conditions imposées. D'une part, une fonction entière à coefficients entiers de plusieurs entiers complexes de K, $\theta = \varphi(\alpha, \beta, \gamma)$ est un nombre de K; si l'on considère les fonctions symétriques élémentaires des conjugués de θ (considéré comme appartenant à K), ces fonctions étant symétriques par rapport séparément aux conjugués de α, de β et de γ, sont des entiers ordinaires et θ est bien un entier complexe. D'autre part, considérons, dans le module de points $\mathcal{R}$, ceux des points $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ qui correspondent aux entiers complexes de K. D'après ce qui précède, ces points forment un sous-module $\mathfrak{E}$ de $\mathcal{R}$; ce module est de dimension n, car si α est un entier complexe élément primitif, le tableau A formé par les n points de $\mathfrak{E}$ correspondant aux n entiers $1, \alpha, (\alpha)^2, \ldots, (\alpha)^{n-1}$ a un déterminant non nul, puisque α est primitif (c'est la racine

carré du discriminant de α. Enfin $\mathfrak{T}$ est type, car les inégalités

$$|\alpha_1| < \varepsilon, \quad |\alpha_2| < \varepsilon, \quad \ldots, \quad |\alpha_n| < \varepsilon$$

entraînent une limitation supérieure pour les fonctions symétriques élémentaires des α_i, qui sont des entiers ; elles ne peuvent donc être vérifiées que par un nombre fini de points de $\mathfrak{T}$. *Donc, tous les entiers complexes d'un corps de degré n se déduisent par addition et soustraction de n d'entre eux.*

Tout tableau de base T *du module* $\mathfrak{T}$, *défini à une équivalence près, est appelé une base des entiers* (1) *du corps.* Le nombre $|\Delta(\mathrm{T})|^2$ qui est une fonction symétrique d'entiers conjugués est un nombre entier positif ou négatif, qu'on appelle le *discriminant du corps.* La raison de cette dénomination est que, si l'on considère un entier complexe α, élément primitif du corps, et le tableau A correspondant, ce tableau étant de $\mathfrak{T}$, on a $\mathrm{A} = \mathrm{ST}$, S à termes entiers; donc $[\Delta(\mathrm{A})]^2$, qui est *le discriminant de* α, *est le produit du discriminant du corps par le carré d'un entier rationnel* (2).

Une base des entiers T est *a fortiori* une base du corps, donc $\Delta(\mathrm{T})$ est réel ou imaginaire et le discriminant $[\Delta(\mathrm{T})]^2$ positif ou négatif suivant la parité de s, nombre de couples de corps imaginaires conjugués parmi les corps conjugués de K. En outre, toute base du corps est le produit à gauche de T par un tableau à termes rationnels, donc de la forme $\left[\frac{1}{d}\right] \times \mathrm{S}$, S à termes entiers, ce qu'on peut écrire

$$\mathrm{H} = \left[\frac{1}{d}\right] \times \mathrm{S} \times \mathrm{T} = (\mathrm{S} \times \mathrm{T}) \times \left[\frac{1}{d}\right],$$

le produit à droite par $\left[\frac{1}{d}\right]$ est une dilatation et $(\mathrm{S} \times \mathrm{T})$ est un tableau du module $\mathfrak{T}$; donc, dans une représentation des nombres du corps par des tableaux, on peut toujours supposer que l'opérateur commun a pour colonnes n systèmes de n entiers conjugués.

---

(1) M. Dedekind appelle base l'ensemble des n entiers auxquels correspondent les points de T.

(2) Dans certains corps, on peut trouver des entiers complexes tels que le tableau A correspondant soit une base des entiers, mais il n'en est pas ainsi en général.

Dans une telle représentation, à tout tableau à termes entiers correspond un entier complexe du corps, puisque l'équation en λ d'un tel tableau est nécessairement de la forme (3). La réciproque n'est pas toujours exacte ([1]), nous verrons au Chapitre suivant une condition nécessaire pour qu'elle le soit; on peut en tous cas montrer déjà que, *si l'opérateur commun des* X *est une base* T *des entiers du corps, à tout entier complexe correspond un tableau à termes entiers* (*et réciproquement*). Supposons qu'il en soit ainsi et que T soit formé des entiers α, β, ..., λ. Alors, si un tableau X correspond à l'entier ω, les lignes de X sont les coordonnées relatives des points de R,

$$(\alpha_1\omega_1, \alpha_2\omega_2, \ldots, \alpha_n\omega_n), \quad (\beta_1\omega_1, \beta_2\omega_2, \ldots, \beta_n\omega_n), \quad \ldots, \quad (\lambda_1\omega_1, \lambda_2\omega_2, \ldots, \lambda_n\omega_n)$$

par rapport à T; les nombres $\alpha\omega$, $\beta\omega$, ..., $\lambda\omega$ étant entiers complexes, ces coordonnées relatives sont entières rationnelles, ce qui démontre le théorème. Dans ce cas, si A_1, A_2, ..., A_n sont les tableaux correspondants aux n entiers de la base T, ou d'une autre base, tout tableau correspondant à un entier complexe du corps est donné par la formule

$$[x_1]A_1 + [x_2]A_2 + \ldots + [x_n]A_n \qquad (x_i \text{ entiers}),$$

et réciproquement.

([1]) Un changement d'opérateur revient, en effet, à remplacer tout tableau X par $X' = PXP^{-1}$, P à termes rationnels. On en déduit aisément que, si X n'est pas un système simple, on peut choisir P de façon que X' ne soit plus à termes entiers. Si l'on considère dans un tel ensemble les tableaux à termes entiers, les entiers complexes correspondants forment un ensemble, inclus dans l'ensemble de tous les entiers, vérifiant les propriétés imposées à $\mathfrak{O}$ et contenant en outre tous les entiers ordinaires (systèmes simples), c'est ce que M. Dedekind appelle un *ordre* et M. Hilbert un *anneau* (*Ring*).

CHAPITRE V.

L'ARITHMÉTIQUE DES ENTIERS D'UN CORPS.

Divisibilité des entiers algébriques.

La définition des entiers complexes est indépendante du corps qui les contient : on peut donc considérer *l'ensemble de tous les entiers complexes algébriques* [1]. Tous les nombres algébriques se déduisent des termes de cet ensemble par division par des entiers ordinaires.

On pourrait espérer étendre l'ensemble des entiers algébriques en y adjoignant les racines d'équations algébriques

$$f(x) = x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_m = 0 \qquad (a_i \text{ entiers complexes}).$$

Mais ceci n'est pas une extension, car *les racines d'une telle équation sont encore des entiers algébriques*. En effet, si l'on considère le corps K, de degré n, défini par les a_i et tous les polynomes $f_1, f_2, \ldots, f_n$ obtenus en remplaçant dans f les coefficients par leurs conjugués dans les n corps conjugués de K, le polynome

$$F(x) = [f_1(x)][f_2(x)]\ldots[f_n(x)]$$

a ses coefficients entiers, son terme de plus haut degré étant x^{mn} ; les zéros de f, étant des zéros de F, sont donc bien des entiers algébriques.

Toutes les propriétés qui, pour les entiers ordinaires, dérivent des propriétés de l'addition, de la soustraction et de la multiplication s'étendent manifestement aussi bien à l'ensemble de tous les entiers complexes qu'à l'ensemble des entiers d'un corps. Il n'en est plus de même de celles qui dérivent de la notion de division

(1) Cet ensemble est dénombrable, de même d'ailleurs que celui des nombres algébriques (*voir* E. Borel, *Leçons sur la théorie des fonctions*) ; nous n'aurons pas besoin pour ce qui suit de ces considérations.

ou de partie entière; cette notion ne se transportant pas aux entiers complexes [1]. En particulier, on ne peut étendre sans précautions, ni même, comme nous le verrons, sans modifications, *les propriétés de divisibilité*.

Nous dirons encore qu'*un entier algébrique* α *est divisible par un entier* β *si le quotient* $\frac{\alpha}{\beta}$, *qui est un nombre algébrique du corps* $K(\alpha, \beta)$, *est aussi un entier complexe;* les mots diviseur et multiple s'étendent d'eux-mêmes. Si, dans l'équation fondamentale d'un entier complexe ε, le terme constant est aussi égal à ± 1, c'est-à-dire si la norme de ε est ± 1, le nombre algébrique $\frac{1}{\varepsilon}$ est encore un entier complexe; il en est de même de $\frac{\alpha}{\varepsilon}$, α entier complexe quelconque. Donc, *tout entier est divisible par un tel entier* ε *qu'on appelle, pour cette raison, une unité complexe.* L'existence des unités complexes est immédiate; on voit, par un raisonnement analogue à celui fait pour l'équation fondamentale d'un entier, qu'il suffit de prendre les racines des équations, irréductibles ou non, à coefficients entiers, ayant ± 1 pour coefficients des termes extrêmes. Nous verrons ultérieurement qu'il en existe aussi, en général, une infinité dans un corps donné.

Dans le cas d'une représentation des entiers complexes d'un corps, par des tableaux à termes entiers, on vérifie la divisibilité d'un entier α correspondant au tableau A par un entier β correspondant à B, en cherchant si AB^{-1} $\left(\text{correspondant à } \frac{\alpha}{\beta}\right)$ est à termes entiers; aux unités correspondent les tableaux de l'ensemble qui sont unimodulaires.

L'existence des unités entraîne une première complication dans l'étude de la divisibilité; si un entier complexe admet un diviseur α, il est aussi divisible par le produit de α par toutes les unités (de l'ensemble de tous les entiers, ou seulement du corps suivant le cas). On peut y obvier partiellement en convenant de ne pas distinguer, au point de vue de la divisibilité (c'est-à-dire

---

(1) Dans le cas des entiers d'un corps, on peut considérer qu'une modification de cette notion est constituée par la propriété indiquée par Hurwitz : *Étant donné un nombre* ρ *d'un corps, on peut trouver un entier complexe* μ *du corps et un entier rationnel* h*, ce dernier limité supérieurement lorsque le corps est déterminé, de façon que la norme de* $h\rho - \mu$ *soit inférieure à* 1.

lorsqu'on emploiera les mots diviseurs ou multiples) entre un entier et son produit par une unité. Ceci convenu, les propriétés de la divisibilité d'une somme ou d'un produit par un entier α, lorsque α divise les deux termes de la somme ou un terme du produit sont encore vraies ainsi que leurs conséquences. Il n'en est plus de même de l'existence ou des propriétés des *nombres premiers*. D'une part, *si l'on envisage l'ensemble de tous les entiers complexes, un entier* ζ (non unité) *a toujours une infinité de diviseurs distincts* (au sens indiqué), par exemple les racines des équations

$$x^m - \zeta = 0.$$

Si, d'autre part, on considère les entiers d'un corps, en raisonnant par exemple sur les tableaux représentatifs, il existe en général (¹) une infinité de tableaux X de l'ensemble tels que AX^{-1} soit à termes entiers. Mais ces tableaux ayant des déterminants au plus égaux à $\Delta(A)$ appartiennent à un nombre fini de systèmes de tableaux équivalents entre eux (Chapitre III). Or, quand deux tels tableaux sont équivalents $X = \Sigma X'$, Σ correspond à un entier du corps qui est nécessairement une unité, donc A n'a qu'un nombre fini de diviseurs distincts; *on peut en conclure l'existence des nombres premiers*, c'est-à-dire *sans diviseurs, autres que les unités du corps ou leurs propres produits par ces unités*. Mais il peut alors arriver qu'un tel nombre premier divise un produit sans diviser aucun des facteurs (²).

La démonstration de la propriété de Gauss sur la décomposition en facteurs d'un polynome à coefficients entiers ne peut donc pas s'étendre. On doit à Kronecker une modification de cette propriété, applicable à l'ensemble des entiers algébriques et dont nous nous servirons par la suite (³) :

Si un polynome

$$F(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \ldots$$

(¹) Sauf le cas du deuxième ordre imaginaire, comme nous le verrons ultérieurement.

(²) On peut sans peine constituer des exemples de ce phénomène. (*Voir* la Note II.)

(³) M. Dedekind a utilisé pour sa théorie des corps algébriques (DIRICHLET-DEDEKIND, *Zahlentheorie*, 4ᵉ édition) un cas particulier de la propriété de Kronecker, l'un des facteurs étant du premier degré.

à coefficients entiers algébriques est décomposé en un produit de deux facteurs $f(x)$, $g(x)$,

$$f(x) = \beta_0 x^n + \beta_1 x^{n-1} + \ldots,$$
$$g(x) = \beta'_0 x^{n'} + \beta'_1 x^{n'-1} + \ldots,$$

tout produit $\beta_i\beta'_j$ d'un coefficient quelconque de f par un coefficient quelconque de g est un entier algébrique.

La propriété est d'abord évidente pour $\beta'_0\beta_0 = \alpha_0$. Désignons par $x_1, x_2, \ldots, x_n$ les zéros de f et par $y_1, y_2, \ldots, y_{n'}$ ceux de g (ce sont des nombres algébriques, zéros de F) et évaluons le produit

$$\frac{\beta_i\beta'_j}{\alpha_0} = \frac{\beta_i}{\beta_0}\frac{\beta'_j}{\beta'_0} = \varphi(x_1, \ldots, x_n)\psi(y_1, \ldots, y_{n'}),$$

c'est une fonction rationnelle entière des zéros de F de degré 1 par rapport à l'un quelconque d'entre eux. Remplaçons alors dans cette expression les x par chaque groupement de n des racines de F et les y par les n' autres racines; l'ordre des racines dans chaque groupement est indifférent puisque φ et ψ sont symétriques. On obtient ainsi $N = C_m^n$ nombres $z_1, z_2, \ldots, z_N$ dont les fonctions symétriques élémentaires sont des fonctions symétriques des zéros de F. Posons

$$\Phi(z) = (z - z_1)(z - z_2)\ldots(z - z_N) = z^N + \delta_1 z^{N-1} + \delta_2 z^{N-2} + \ldots,$$

δ_i est une fonction symétrique entière de degré i, des zéros de F, donc une fonction entière de degré i des quotients $\frac{\alpha_k}{\alpha_0}$, donc encore le quotient d'un entier algébrique par $(\alpha_0)^i$. On peut alors écrire $\Phi(z)$

$$\Phi(z) = z^N + \frac{\gamma_1}{\alpha_0} z^{N-1} + \frac{\gamma_2}{(\alpha_0)^2} z^{N-2} + \ldots + \frac{\gamma_N}{(\alpha_0)^N},$$

$\frac{\beta_i\beta'_j}{\alpha_0}$ est un zéro de ce polynome et $\beta_i\beta'_j$ est un zéro du polynome en y,

$$(\alpha_0)^N \Phi\left(\frac{y}{\alpha_0}\right) = y^N + \gamma_1 y^{N-1} + \gamma_2 y^{N-2} + \ldots + \gamma_N,$$

les γ étant des entiers complexes, tout zéro de ce polynome est un entier complexe et la proposition est démontrée ([1]).

Une conséquence immédiate de ce théorème est que tout entier complexe diviseur commun des coefficients α de F est aussi un diviseur de tous les produits $\beta_i\gamma_j$. Remarquons encore, comme pour le théorème de Gauss, que la même propriété s'étend au cas d'un polynome à plusieurs variables produit de deux polynomes.

Idéaux d'un corps.

Revenons à l'ensemble des entiers d'un corps K(ω), soit ϖ le module type de points correspondants et T une base de ϖ. Considérons ainsi que nous l'avons fait au Chapitre II pour le plus grand commun diviseur des entiers ordinaires, plusieurs entiers déterminés du corps, α, β, ..., même en nombre infini, et *l'ensemble de tous les entiers de* K

$$x\alpha + y\beta + \ldots, \tag{1}$$

obtenus en remplaçant x, y, ... *par tous les entiers de* K. Cet ensemble n'est plus nécessairement identique à l'ensemble des multiples d'un entier complexe. M. Dedekind a tourné la difficulté en attribuant à ces êtres une existence propre et en étudiant leur arithmétique ([2]); nous avons déjà fait une convention analogue pour les entiers ordinaires en représentant par $(a, b, \ldots)$ l'ensemble des multiples du plus grand commun diviseur de a, b, ... Même dans le cas d'un corps, où tous les ensembles précédents seraient identiques à des ensembles de multiples, il y aurait encore intérêt à considérer de tels ensembles plutôt que les diviseurs communs de leurs termes, car ces diviseurs ne sont définis qu'au produit près par les unités du corps. Un tel ensemble est appelé *un idéal* et désigné par

$$\alpha, \beta, \ldots.$$

([1]) Cette démonstration est due à M. Hurwitz (*Gött. Nachr.*, 1895). On trouvera d'autres démonstrations intéressantes du même théorème dans le livre de J. König, *Einleitung in die allgemeine Theorie der algebraischen Grössen*.

([2]) Kummer avait imaginé d'admettre pour les nombres d'un tel ensemble l'existence d'un *facteur commun idéal*, idéal étant pris au sens ordinaire du mot.

pour rappeler les entiers qui servent à le définir. En n'explicitant pas ces entiers, *on peut encore définir un idéal d'un corps, un ensemble d'entiers complexes de ce corps, tels que :*

1° *Cet ensemble contienne le produit de l'un quelconque de ses termes par tout entier du corps;*

2° *Il contienne la somme et la différence de deux quelconques de ses termes.*

Un idéal est dit *principal* et désigné par $[\omega]$, conformément à la notation précédente, s'il se confond avec l'ensemble des multiples de ω; ω n'est alors défini qu'à un produit près par une unité. Dans le cas où ω est lui-même une unité, l'idéal qu'on peut désigner par $[1]$ est confondu avec l'ensemble des entiers du corps; pour qu'il en soit ainsi, il suffit de vérifier qu'il contient une unité.

Si à chaque entier β de l'idéal nous faisons correspondre le point $(\beta_1, \beta_2, \ldots, \beta_n)$ on obtient, d'après la deuxième condition, un sous-module $\mathcal{A}$ de $\mathcal{E}$. Ce module est de dimension n, car d'après la première propriété, le tableau

$$T = [\beta_1, \beta_2, \ldots, \beta_n],$$

de déterminant non nul, est formé de points de $\mathcal{A}$; donc $\mathcal{A}$ est type, sa base est de la forme $P \times T$ (P à termes rationnels, défini à une équivalence près), et tous ses points sont donnés par la formule

$$\| \beta_1 \quad \beta_2 \quad \ldots \quad \beta_n \| = \| x_1 \quad x_2 \quad \ldots \quad x_n \| \times PT \quad (x \text{ entiers rationnels}),$$

un idéal peut donc être considéré comme défini au plus par n nombres. Nous dirons que P est une base relative de l'idéal, c'est en effet une base du module lorsque l'on considère des coordonnées relatives à T; on peut toujours supposer que P a été mis sous la forme réduite d'Hermite.

Ce n'est pas un tableau quelconque, et il n'est pas sans intérêt d'en donner une propriété caractéristique : *pour qu'un tableau de* $\mathcal{E}$, *donc de la forme* $P \times T$, *soit une base d'un idéal de* K, *il faut et il suffit que tous les tableaux*

$$(PT)[\alpha_1, \alpha_2, \ldots, \alpha_n](PT)^{-1} \qquad (\alpha \text{ entier de } K)$$

soient à termes entiers rationnels, c'est-à-dire encore qu'en prenant PT pour opérateur d'une représentation des nombres d'un corps par des tableaux, à tous les entiers complexes correspondent des tableaux à termes entiers. Exprimons que le produit d'un entier de l'idéal par un entier du corps est encore un entier de l'idéal, il suffit d'écrire cette égalité pour les matrices de type (1, n) correspondant à chacun de ces entiers. Il faut que, quels que soient les entiers rationnels x_i, il leur corresponde des entiers y_i tels que

$$(2)\qquad \| x_1 \ x_2 \ \dots \ x_n \| \times PT[\alpha_1, \alpha_2, \dots, \alpha_n] = \| y_1 \ y_2 \ \dots \ y_n \| \times PT$$

ou

$$(2\,bis)\qquad \| x_1 \ x_2 \ \dots \ x_n \| \times PT[\alpha_1, \dots, \alpha_n](PT)^{-1} = \| y_1 \ y_2 \ \dots \ y_n \|.$$

Ceci exige que le tableau du premier membre soit à termes entiers rationnels, quel que soit l'entier α du corps.

Réciproquement, si l'on a une représentation des entiers complexes par des tableaux à termes entiers, on peut supposer que l'opérateur est un tableau PT de $\mathfrak{T}$. Alors, quels que soient les entiers rationnels x et l'entier α du corps, il leur correspond des entiers y définis par l'égalité (2 *bis*), et par conséquent vérifiant l'égalité (2). Donc, aux points du module de base PT correspondent des entiers du corps vérifiant les deux conditions de définition d'un idéal.

La propriété précédente conduit à un moyen pratique de recherche des idéaux d'un corps ou plutôt de leurs bases relatives. En supposant toujours que l'opérateur est une base des entiers et en considérant les n tableaux A_i correspondant aux n entiers d'une base, il suffit de chercher tous les tableaux P à termes entiers, définis à une équivalence près, mis par exemple sous la forme réduite d'Hermite, et tels que

$$PA_1P^{-1}, \quad PA_2P^{-1}, \quad \dots, \quad PA_nP^{-1},$$

soient à termes entiers ; il en sera de même de tout Tableau

$$PAP^{-1} = P([x_1]A_1 + [x_2]A_2 + \dots + [x_n]A_n)P^{-1},$$

A correspondant à un entier quelconque du corps. On peut encore indiquer une condition, moins pratique, pour qu'un idéal donné

par une base relative P soit principal. Pour un tel idéal $[\omega]$ on a immédiatement une base qui est $T \times [\omega_1, \omega_2, \ldots, \omega_n]$. Donc, pour que l'idéal de base PT soit principal, il faut et il suffit

$$PT \text{ équivalent à } T[\omega_1, \omega_2, \ldots, \omega_n]$$

ou

$$P \text{ équivalent à } T[\omega_1, \ldots, \omega_n]\, T^{-1},$$

c'est-à-dire que P doit être équivalent à un tableau du corps et réciproquement.

En se laissant guider par l'analogie avec les ensembles de multiples dans l'arithmétique des entiers ordinaires, on est conduit sans peine à la notion de divisibilité des idéaux. Si un entier ordinaire a est divisible par b, l'ensemble des multiples de a est contenu dans l'ensemble des multiples de b; nous dirons par extension *qu'un idéal $\mathcal{A}$ est divisible par un idéal $\mathcal{B}$, si tous les nombres, ou points, de $\mathcal{A}$ sont contenus dans $\mathcal{B}$*. C'est dire que $\mathcal{A}$ est un sous-module de $\mathcal{B}$, on en déduit immédiatement (Chap. II) une relation entre leurs bases relatives P et T, il faut et il suffit que

$$P = SQ, \qquad S = PQ^{-1} \text{ à termes entiers.}$$

Nous dirons encore que $\mathcal{A}$ est multiple de $\mathcal{B}$ et $\mathcal{B}$ diviseur de $\mathcal{A}$; manifestement tout multiple de $\mathcal{B}$ est aussi multiple de tout diviseur de $\mathcal{B}$. Un idéal admet au moins comme diviseur lui-même et l'idéal $[1]$; il ne peut en avoir qu'un nombre fini, car les tableaux X à termes entiers tels que PX^{-1} soient à termes entiers ont leur déterminant limité [inférieur en valeur absolue à $|\Delta(P)|$] et par conséquent se répartissent en un nombre fini de systèmes (Chap. III). On en déduit, comme en arithmétique ordinaire, *l'existence d'idéaux premiers, c'est-à-dire d'idéaux n'ayant d'autres diviseurs qu'eux-mêmes et l'idéal* $[1]$. Au contraire, il existe une infinité de multiples d'un idéal $\mathcal{A}$; tous les idéaux principaux $[\alpha]$, α étant un entier de $\mathcal{A}$, ont leurs termes contenus dans $\mathcal{A}$, donc sont des multiples de $\mathcal{A}$.

On peut étendre aux idéaux *les propriétés du plus petit multiple commun et du plus grand commun diviseur* de plusieurs nombres. Soient plusieurs idéaux en nombre fini $\mathcal{A}$, $\mathcal{B}$, ..., il y a des entiers communs à tous ces idéaux, par exemple les produits $\alpha\beta$, ..., d'entiers appartenant respectivement à $\mathcal{A}$, $\mathcal{B}$, ... Tous

ces entiers forment un idéal $\mathfrak{M}$, la différence de deux d'entre eux, ou le produit de l'un par un entier du corps étant encore un entier commun à $\mathfrak{A}$, $\mathfrak{B}$, ... Cet idéal $\mathfrak{M}$ joue le rôle de plus petit multiple commun, car tout idéal $\mathfrak{M}'$ multiple commun de $\mathfrak{A}$, $\mathfrak{B}$, ..., ayant ses entiers inclus à la fois dans $\mathfrak{A}$, $\mathfrak{B}$, ... les a aussi inclus dans $\mathfrak{M}$, c'est dire que $\mathfrak{M}'$ est multiple de $\mathfrak{M}$; réciproquement, $\mathfrak{M}'$ multiple de $\mathfrak{M}$ l'est aussi de ses diviseurs $\mathfrak{A}$, $\mathfrak{B}$, ... Considérons encore l'idéal $\mathfrak{D}$ défini par les entiers des bases de $\mathfrak{A}$, $\mathfrak{B}$, ..., cet idéal, qui peut être [1] joue le rôle de plus grand commun diviseur. En effet, tout diviseur commun de $\mathfrak{A}$, $\mathfrak{B}$, ... contenant les entiers de ces idéaux contient les entiers de $\mathfrak{D}$, et est un diviseur de $\mathfrak{D}$; la réciproque est évidente. *Si le plus grand commun diviseur est* [1] *on dit encore que les idéaux sont premiers dans leur ensemble, ils n'ont aucun diviseur commun sauf* [1].

Nous avons vu au Chapitre III que certaines notions de divisibilité peuvent s'étendre aux fractions. Il en est de même pour les corps algébriques et l'on peut dans l'ensemble (1) remplacer les entiers α, β, ... (supposés toutefois en nombre fini) par des nombres du corps quelconques

$$\frac{\alpha}{a}, \quad \frac{\beta}{b}, \quad \dots \qquad \left(\begin{array}{l}\alpha, \beta, \dots \text{ entiers de K} \\ a, b, \dots \text{ entiers rationnels}\end{array}\right);$$

les x restant toujours des entiers arbitraires de K. Nous appellerons un tel ensemble *idéal fractionnaire;* il vérifie encore les propriétés I et II. Ses termes $\varpi = \frac{\omega}{d}$ sont des quotients d'entiers complexes ω du corps par des entiers rationnels d, limités supérieurement en valeur absolue (au plus égaux au plus petit multiple commun de $|a|$, $|b|$). Il en résulte que les points correspondants $(\varpi_1, \dots, \varpi_n)$ forment encore un module type : les inégalités $|\varpi_i| < \varepsilon$ entraînent, puisque les d sont limités, une limitation supérieure pour les fonctions symétriques élémentaires des ω, fonctions qui sont des entiers rationnels; il n'y a donc qu'un nombre fini de solutions. Le même raisonnement que pour les idéaux ordinaires montre que ce module est de dimension n et tous ses points sont encore donnés par

$$\| \varpi_1 \quad \dots \quad \varpi_n \| = \| x_1 \quad \dots \quad x_n \| \times \text{RT} \qquad (x \text{ entiers rationnels}),$$

la base relative R définie à une équivalence près étant cette fois à termes rationnels, non nécessairement entiers. La propriété caractéristique de la base relative subsiste, de même que la condition pour que *l'idéal fractionnaire soit principal, c'est-à-dire identique à l'ensemble des multiples d'un nombre de* K. Il en est de même de la définition de la divisibilité et des propriétés du plus grand commun diviseur et du plus petit multiple commun de plusieurs idéaux fractionnaires, mais il ne suffit plus qu'un idéal contienne une unité pour être confondu avec [1], on peut affirmer alors seulement qu'il contient tous les entiers du corps et que *sa base relative est l'inverse d'un tableau à termes entiers* (1).

Décomposition des idéaux en facteurs.

On peut pousser plus loin l'analogie de l'arithmétique des idéaux d'un corps avec l'arithmétique des nombres ordinaires, en montrant la possibilité de décompositions en facteurs. Il est nécessaire pour cela de définir la multiplication des idéaux : *étant donnés deux idéaux* $\mathcal{A}$ *et* $\mathcal{B}$ (entiers ou fractionnaires) *on appelle produit* $\mathcal{A}\mathcal{B}$, *l'idéal défini par tous les produits des termes de* $\mathcal{A}$ *par les termes de* $\mathcal{B}$.

Pour définir $\mathcal{A}\mathcal{B}$ il suffit évidemment de considérer le produit de chaque élément d'un système d'éléments en nombre fini α, β, ... définissant $\mathcal{A}$ (par exemple les n nombres d'une base) par chaque élément d'un système α', β', ... définissant $\mathcal{B}$; car le produit d'un nombre quelconque de $\mathcal{A}$ par un nombre quelconque de $\mathcal{B}$

$$(x\alpha + y\beta + \ldots)(x'\alpha' + y'\beta' + \ldots)$$

est compris *a fortiori* dans la formule

$$x''\alpha\alpha' + y''\alpha\beta' + z''\beta\alpha' + \ldots.$$

Donc $\mathcal{A}\mathcal{B}$ défini par un nombre fini d'éléments est bien un idéal (ceci pour le cas de $\mathcal{A}\mathcal{B}$ fractionnaire).

La multiplication des idéaux est manifestement univoque, asso-

(1) Un tel idéal est en effet un diviseur de l'idéal [1] et sa base relative R devant diviser le système simple [1], R^{-1} est à termes entiers.

ciative et commutative

$$(\mathcal{A}\mathcal{B})\mathcal{C} = \mathcal{A}(\mathcal{B}\mathcal{C}), \qquad \mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A};$$

le produit d'un idéal $\mathcal{A} = (\alpha, \beta, \ldots)$ par un idéal principal $[\omega]$, (qu'on note quelquefois $\omega\mathcal{A}$) est $(\omega\alpha, \omega\beta, \ldots)$ et est formé des produits par ω des nombres de $\mathcal{A}$; en particulier le produit de deux idéaux principaux $[\alpha]$, $[\beta]$ est l'idéal principal $[\alpha\beta]$. L'idéal $[1]$ vérifie l'équation

$$\mathcal{A}\mathcal{X} = \mathcal{A}.$$

Nous allons montrer que c'est le seul et établir en même temps la possibilité et l'unicité de l'opération inverse de la multiplication. Il nous suffira pour cela d'établir *l'existence d'un et un seul idéal $\mathcal{A}^{-1}$, inverse d'un idéal donné $\mathcal{A}$, c'est-à-dire tel que*

$$\mathcal{A}\mathcal{A}^{-1} = [1].$$

Supposons $\mathcal{A}$ défini par les nombres α, β, ... de K et considérons la forme qui sera dite *contenant l'idéal*

$$\varphi(x, y, \ldots) = \alpha x + \beta y + \ldots,$$

et les n formes φ_1, φ_2, ..., φ_n, dont l'une est identique à φ, obtenues en remplaçant α, β, ... par leur conjugués. Leur produit, qui, par analogie avec le cas d'un nombre du corps, peut s'appeler *la norme de la forme* φ

$$N(\varphi) = \Phi(x, y, \ldots) = \varphi_1\varphi_2\ldots\varphi_n,$$

est un polynome de degré n à coefficients rationnels; appelons $\frac{p}{q}$ le plus grand commun diviseur de ces coefficients; $\Phi_1 = \frac{q}{p}\Phi$ est un polynome primaire, il est divisible par φ et le quotient ψ de degré $n-1$ a ses coefficients dans K puisqu'ils se déduisent par des opérations rationnelles de ceux de Φ_1 et de φ: ces coefficients α', β', ... définissent un idéal $\mathcal{A}^{-1}$ qui répond précisément à la question. En effet

$$\mathcal{A}\mathcal{A}^{-1} = (\alpha\alpha', \alpha\beta', \beta\alpha', \ldots);$$

or d'après le théorème de Kronecker appliqué à Φ_1, qui est à coefficients entiers rationnels, tous les produits de la parenthèse sont des entiers complexes, donc $\mathcal{A}\mathcal{A}^{-1}$ est un idéal entier;

d'autre part, cet idéal contient tous les coefficients de Φ_1 et par conséquent 1 qui en est une combinaison linéaire à coefficients entiers, puisqu'ils sont premiers entre eux; donc $\mathcal{A}\mathcal{A}^{-1} = [1]$. Cet inverse est unique car si un idéal $\mathcal{A}'$ est tel que $\mathcal{A}\mathcal{A}' = [1]$, on a la suite d'égalités évidentes

$$\mathcal{A}' = \mathcal{A}'[1] = \mathcal{A}'(\mathcal{A}\mathcal{A}^{-1}) = (\mathcal{A}'\mathcal{A})\mathcal{A}^{-1} = \mathcal{A}^{-1}.$$

Si $\mathcal{A}$ est un idéal principal $[\varpi]$, l'inverse est $\left[\frac{1}{\varpi}\right]$. Si $\mathcal{A}$ est entier, l'inverse $\mathcal{A}^{-1}$ contient tous les entiers du corps, *et sa base relative est l'inverse d'un tableau à termes entiers*. Réciproquement, si l'on considère un idéal $\mathcal{A}'$ contenant une unité et dont la base relative est par conséquent de la forme précédente, tout nombre de l'inverse de $\mathcal{A}'$, multiplié par 1 qui est dans $\mathcal{A}'$, doit donner un entier complexe; donc cet inverse composé d'entiers est un idéal entier.

Du fait de l'existence et de l'unicité de l'inverse, on déduit immédiatement l'existence et l'unicité du quotient de $\mathcal{A}$ par $\mathcal{B}$, c'est-à-dire de la solution de l'équation

$$\mathcal{B}\mathcal{X} = \mathcal{A}, \qquad \text{équivalente à} \qquad \mathcal{X} = \mathcal{A}\mathcal{B}^{-1}.$$

Appliquons les résultats précédents à la divisibilité des idéaux entiers ou fractionnaires. On a, entre cette notion définie *a priori*, et celle du produit la relation qui complète l'analogie avec la divisibilité des entiers : *si le quotient d'un idéal $\mathcal{A}$ par un idéal $\mathcal{B}$ est un idéal entier $\mathcal{C}$, $\mathcal{A}$ est divisible par $\mathcal{B}$; et réciproquement si $\mathcal{A}$ est divisible par $\mathcal{B}$, le quotient de $\mathcal{A}$ par $\mathcal{B}$ est un idéal entier*. Si $\mathcal{A} = \mathcal{B}\mathcal{C}$, tous les nombres de $\mathcal{A}$ sont manifestement contenus dans $\mathcal{B}$ puisque produits de termes de $\mathcal{B}$ par certains entiers complexes (appartenant à $\mathcal{C}$). Si, réciproquement, les nombres d'un idéal $\mathcal{A}$ sont dans $\mathcal{B}$, le produit $\mathcal{A}\mathcal{B}^{-1}$ est contenu dans $\mathcal{B}\mathcal{B}^{-1}$ et c'est un idéal entier $\mathcal{C}$.

L'application au plus grand commun diviseur et au plus petit multiple commun est immédiate, *la condition nécessaire et suffisante pour que $\mathcal{M}$, ou $\mathcal{D}$, soit le plus petit multiple commun ou le plus grand commun diviseur des idéaux $\mathcal{A}$, $\mathcal{B}$, ... est que les quotients $\mathcal{M}\mathcal{A}^{-1}$, $\mathcal{M}\mathcal{B}^{-1}$, ... ou $\mathcal{A}\mathcal{D}^{-1}$, $\mathcal{B}\mathcal{D}^{-1}$, ..., soient des idéaux entiers premiers entre eux*. Démontrons-le, par

exemple pour $\mathfrak{M}$, si $\mathfrak{M}\mathfrak{A}^{-1}$, $\mathfrak{M}\mathfrak{B}^{-1}$, ... n'étaient pas premiers, ils auraient un diviseur $\mathfrak{Q}$ et $\mathfrak{M}\mathfrak{Q}^{-1}$ serait un idéal multiple commun de $\mathfrak{A}$, $\mathfrak{B}$, ..., puisque $(\mathfrak{M}\mathfrak{Q}^{-1})\mathfrak{A}^{-1}$, $(\mathfrak{M}\mathfrak{Q}^{-1})\mathfrak{B}^{-1}$, ... seraient des idéaux entiers; réciproquement tout multiple commun autre que le plus petit est de la forme $\mathfrak{Q}\mathfrak{M}$ et ses quotients par $\mathfrak{A}$, $\mathfrak{B}$, ... admettent $\mathfrak{Q}$ pour commun diviseur, et ne sont pas premiers. La même démonstration s'étend à $\mathfrak{D}$; la propriété a une plus grande importance que pour les entiers rationnels, la notion de quotient étant cette fois postérieure à celle de divisibilité, et c'est du théorème précédent qu'on déduit

$$\mathfrak{Q} \times \text{p. g. c. d.}(\mathfrak{A}, \mathfrak{B}, \ldots) = \text{p. g. c. d.}(\mathfrak{A}\mathfrak{Q}, \mathfrak{B}\mathfrak{Q}, \ldots),$$
$$\mathfrak{Q} \times \text{p. p. m. c.}(\mathfrak{A}, \mathfrak{B}, \ldots) = \text{p. p. m. c.}(\mathfrak{A}\mathfrak{Q}, \mathfrak{B}\mathfrak{Q}, \ldots).$$

Les conséquences sont ensuite les mêmes que pour les nombres rationnels et je renvoie au Chapitre III pour quelques-unes d'entre elles, aux traités élémentaires d'arithmétique ou de théorie des nombres pour les autres.

Les propriétés et démonstrations spéciales (¹) à la divisibilité des nombres se transportent ainsi aux idéaux : diverses expressions d'un idéal fractionnaire comme quotient d'idéaux entiers, idéaux premiers, ... En particulier *un idéal entier est décomposable d'une seule façon en un produit d'idéaux premiers.*

(¹) Il y a exception toutefois pour l'existence d'une infinité d'idéaux premiers, il faut alors modifier la démonstration habituelle; il en est de même pour toutes les propriétés où intervient la notion de somme de nombres (par exemple les congruences et le théorème de Fermat), cette notion ne se transportant pas aux idéaux (*voir* la Note III).

CHAPITRE VI.

RÉDUCTION CONTINUELLE ET THÉORÈMES DE MINKOWSKI.

Tableaux réduits d'un système.

Pour avancer plus loin dans cette théorie des entiers des corps algébriques et des idéaux, il est utile et même nécessaire d'étudier d'un peu plus près les systèmes de tableaux, notamment pour les relations entre les différentes bases d'un idéal et la recherche des unités. Nous avons étudié au Chapitre III les systèmes de tableaux à termes entiers et même fractionnaires et nous avons montré que dans un tel système existait un et un seul tableau d'une forme particulièrement simple (forme réduite d'Hermite). Une pareille circonstance se présente-t-elle dans le cas général et dans un système de tableaux peut-on distinguer un ou plusieurs tableaux particulièrement simples ou remarquables? D'une façon précise peut-on donner une définition (¹) des *tableaux réduits d'un système* telle que : cette définition soit indépendante du tableau particulier qui a servi à définir le système; dans tout système il existe au moins un tableau réduit et, s'il y en a une infinité, on puisse les classer dans un ordre déterminé et également indépendant du tableau qui a servi à définir le système?

Avant de chercher une telle définition il n'est peut-être pas inutile d'en rappeler l'utilité. D'une part elle peut servir à constater l'équivalence ou la non-équivalence de deux tableaux donnés A et B; il suffira de former respectivement les tableaux réduits des systèmes constitués par les tableaux équivalents à A et à B et

(¹) On pourrait particulariser et définir seulement les tableaux réduits des systèmes d'une certaine catégorie et non de tous les systèmes simultanément. Il ne semble pas qu'il y aurait un grand avantage, exception faite, bien entendu, des tableaux à termes entiers.

de chercher si les ensembles ainsi obtenus sont identiques ou non, (on voit pour cela la nécessité de bien ordonner ces ensembles). D'autre part, soit à trouver tous les systèmes vérifiant certaines conditions, se traduisant par une même condition pour les tableaux (par exemple un déterminant donné), il suffira de chercher tous les tableaux réduits vérifiant cette condition.

Supposons d'abord que chaque système envisagé soit défini par un de ses tableaux T d'ordre n. On peut considérer le système défini par T comme constitué par l'ensemble des bases d'un module type $\mathfrak{T}$ de points. Tout revient alors à chercher une base ou encore un tableau remarquable de $\mathfrak{T}$, car en suivant la marche donnée dans la démonstration du théorème fondamental, on peut déduire d'un tel tableau une base et même une seule base. Une intuition simple peut conduire à la définition d'un tel tableau : pour l'espace à une dimension la question ne se pose pas, pour le plan (réel) un tableau, à l'ordre près des lignes, définit un triangle $\mathrm{OA_1A_2}$ et réciproquement en adoptant un ordre pour les côtés. On aura un tableau remarquable, ou au plus un nombre fini, en cherchant celui ou ceux de ces triangles dont les côtés issus de O sont les plus petits possibles et en adoptant pour ordre des côtés l'ordre de grandeur. De même pour l'espace (réel) on peut prendre le tétraèdre $\mathrm{OA_1A_2A_3}$ qui a les plus petits côtés, et ainsi de suite, on étend sans difficulté aux espaces à n dimensions réels ou semi-réels.

Traduisons en langage algébrique; pour comparer les côtés adoptons pour expression de la distance une distance généralisée quelconque, soit $S(\mathrm{OM})$. Ceci convenu on peut énoncer le résultat prévu géométriquement :

Dans tout module type de dimension n, il existe toujours un nombre fini (non nul) de tableaux V, $\Delta(\mathrm{V}) \neq 0$, *formés de points* $\mathrm{A_1}, \mathrm{A_2}, \mathrm{A_3}, \ldots, \mathrm{A}_n$ *tels que*

$$(1)\quad \left\{\begin{array}{ll} S(\mathrm{OA}) \geqq S(\mathrm{OA_1}) & (\mathrm{A} \text{ quelconque de } \mathfrak{T}), \\ S(\mathrm{OA}) \geqq S(\mathrm{OA_2}) & (\mathrm{A} \text{ de } \mathfrak{T} \text{ et non de } \mathrm{OA_1}), \\ S(\mathrm{OA}) \geqq S(\mathrm{OA_3}) & (\mathrm{A} \text{ de } \mathfrak{T} \text{ et non de } \mathrm{OA_1A_2}), \\ \ldots\ldots & \ldots\ldots \end{array}\right.$$

en particulier

$$(1\ bis)\quad S(\mathrm{OA_1}) \geqq S(\mathrm{OA_2}) \geqq \ldots \geqq S(\mathrm{OA}_n);$$

on a désigné pour abréger par oA_1, oA_1A_2, ... les espaces à 1, 2, ... dimensions définis par o et A_1; o, A_1 et A_2; .... On peut trouver un point A_1 de $\mathfrak{T}$ tel que $S(oA_1)$ soit minimum, il suffit de le choisir parmi les points A de $\mathfrak{T}$, en nombre fini, vérifiant

$$S(oA) \leqq S(oB),$$

B étant un point de $\mathfrak{T}$. S'il y a plusieurs solutions, on choisit l'une d'elles; on peut déterminer de même un point A_2 de $\mathfrak{T}$, n'appartenant pas au sous-espace oA_1 et tel que $S(oA_2)$ soit le plus petit possible, et ainsi de suite jusqu'à n points qui forment un tableau V à déterminant non nul. Comme il n'y a hésitation chaque fois qu'entre un nombre fini de points, en envisageant tous les cas possibles, on n'obtient qu'un nombre fini de tableaux V, nous les appellerons *tableaux minima*, et $S(oA_1)$, $S(oA_2)$, ..., $S(oA_n)$ seront dits *un système de distances minima.*

De chaque tableau minimum V ainsi obtenu, on peut, comme nous l'avons dit, en suivant la méthode indiquée dans la démonstration du théorème général (Chap. II et III) déduire une et une seule base U de $\mathfrak{T}$ (peut-être identique à V)

$$U = SV$$

(S à termes fractionnaires de la forme réduite d'Hermite). Les tableaux U sont équivalents à T, leur définition est indépendante du tableau T choisi pour définir ce système; nous dirons que ce sont *les tableaux réduits du système* [1].

Nous verrons plus tard comment on peut fixer en général une limite inférieure aux termes de S (leur limite supérieure est 1). Dans le cas du deuxième ordre, cette limite est $\frac{1}{2}$ et il existe au moins un tableau minimum qui soit une base. Considérons le tableau équivalent et peut-être identique à S

$$S_1 = \begin{Vmatrix} a_1 & 0 \\ b_1 & b_2 \end{Vmatrix}.$$

ayant mêmes termes que S dans la diagonale principale, mais tel que $|b_1|$ soit au plus égal à $\frac{a_1}{2}$. Soient A'_1, A'_2 les points de $S_1 \times V$

---

[1] Il n'est pas sans intérêt de remarquer que cette démonstration non seulement prouve l'existenee des tableaux réduits, mais encore fournit un moyen de les calculer par des opérations en nombre fini.

qui est encore une base de $\mathfrak{S}$. On a

$$A'_1 = a_1 A_1, \qquad S(OA'_1) = a_1 S(OA_1).$$

Comme $S(OA_1)$ est un minimum, il est impossible que a_1 soit inférieur à 1 et A'_1 est identique à A_1. On a ensuite

$$A'_2 = b_1 A_1 + b_2 A_2, \qquad S(OA'_2) \leq |b_1| S(OA_1) + b_2 S(OA_2) \leq (|b_1| + b_2) S(OA_2);$$

or $|b_1|$ est au plus égal à $\frac{1}{2}$, b_2 est donc au moins égal à $\frac{1}{2}$, sinon $S(OA'_2)$ serait inférieur à $S(OA_2)$. Comme b_2 est l'inverse d'un nombre entier, il est égal, soit à 1 et alors V est une base ; soit à $\frac{1}{2}$, il en est alors de même de $|b_1|$ [sinon $S(OA'_2) < S(OA_2)$], et $S(OA'_2) = S(OA_2)$. Il en résulte que S_1 · V qui est une base est un tableau minimum. Ce second cas ne se présentera pas si l'une des inégalités conditionnelles précédentes devient une véritable inégalité, ceci se passe notamment pour une distance généralisée dont le corps caractéristique est *partout convexe;* il ne se présentera pas non plus si l'on sait à l'avance qu'il n'y a qu'un seul tableau minimum (¹).

Dans ce que nous avons dit jusque maintenant, nous n'avons pas spécifié la distance généralisée choisie. En adoptant par exemple la spanne à $r+s$ paramètres pour des valeurs déterminées des λ_i, μ_j,

$$S(OM) = \text{maximum}\,(\lambda_i|\xi_i|, \mu_j|\eta_j|),$$

on peut chercher à diminuer le nombre de tableaux réduits; il suffit d'ajouter des conditions supplémentaires pour la définition des tableaux V. Remarquons d'abord que chaque point A_i d'un tel tableau V peut être remplacé par son symétrique par rapport à l'origine, $-A_i$; nous pouvons faire un choix entre les deux points, en convenant par exemple de ne considérer que celui dont la première coordonnée est positive (²), si elle est réelle et non nulle. Il peut encore se faire qu'il y ait indécision dans l'ordre des lignes

(¹) On peut remarquer que le raisonnement précédent s'appliquerait encore, dans le cas du $n^{\text{ième}}$ ordre, au mineur formé par les deux premières lignes et colonnes de S.

(²) On pourrait faire un choix analogue, si elle était imaginaire, en considérant sa partie réelle mais nous verrons que cela aurait moins d'intérêt au point de vue où nous aurons à nous placer dans la suite.

consécutives de X lorsque les points de ces lignes sont à une même spanne de l'origine, ou encore sont des *minima simultanés*. Dans ce cas nous distinguerons le *rang de chaque spanne*, c'est-à-dire le rang de la coordonnée à laquelle elle est égale et nous rangerons les points dans le même ordre que le rang minimum de ces spannes; il n'y aura plus indécision que si plusieurs de ces spannes sont de même rang (¹). On peut écrire ces nouvelles conditions

$$(2) \qquad p_1^i > 0, \qquad X_i = (p_1^i, p_2^i, \ldots, p_n^i),$$

$$(2\ bis) \qquad \left\{ \begin{array}{l} \text{si } S(OX_i) = S(OX_{i+1}), \\ \text{rang } S(OX_i) < \text{rang } S(OX_{i+1}). \end{array} \right.$$

Ces conditions conduisent à un résultat particulièrement simple si T est à termes réels et s'il n'y a pas de relation linéaire homogène à coefficients entiers entre les termes d'une même colonne de T. Alors la donnée de la $i^{\text{ème}}$ coordonnée d'un point de $\mathfrak{C}$ entraîne la connaissance de ce point, chaque ligne de V est bien déterminée et il n'y a dans ce cas *qu'un seul tableau réduit*.

Réduction continuelle pour le deuxième ordre.

La définition des tableaux réduits par les conditions (1), (2) et (2 *bis*) convient dans tous les cas où le tableau est bien déterminé, c'est ce qui se présentait en particulier dans les recherches de MM. Jordan et Poincaré sur les formes à coefficients entiers. Mais il peut arriver qu'un tableau ne soit défini qu'à une dilatation près. C'est le cas si l'on considère les tableaux auxquels une forme décomposable est associée ou encore les opérateurs d'un tableau donné à termes réels. Il faut alors chercher à définir dans le système de tableaux équivalents à T un *ensemble réduit de tableaux*, vérifiant les conditions énoncées au début du Chapitre, *et tel en outre que, si l'on fait sur* T *une dilatation, on obtienne l'ensemble réduit du nouveau système en faisant la même dilatation sur les tableaux de l'ancien ensemble.*

(¹) Si ces spannes sont de même rang on pourrait classer les points, en considérant les points d'un espace à $n-1$ ou $n-2$ dimensions obtenus en supprimant les coordonnées de rang i, et s'il y a lieu, leurs imaginaires conjuguées et en classant les nouveaux points suivant les grandeurs de leurs spannes.

Un procédé immédiat pour avoir un tel ensemble réduit est de prendre tous les tableaux U équivalents à T tels que, pour une certaine dilatation E, le tableau UE équivalent à TE soit réduit au sens indiqué précédemment. En effet, si l'on remplace T par TE_1 le tableau UE_1 est encore susceptible de devenir réduit pour la dilatation EE_1^{-1} et réciproquement; l'ensemble correspondant à TE_1 se déduit donc de l'ensemble correspondant à T par la dilatation E_1. Il est nécessaire en outre de montrer que l'ensemble ainsi défini est susceptible d'être ordonné et que ce rangement ne change pas si l'on fait une dilatation sur T. Avant d'aborder l'étude de tels ensembles dans le cas général examinons le cas particulier des tableaux du deuxième ordre.

Cas imaginaire. — Soit d'abord T formé de deux colonnes imaginaires conjuguées

$$T = \left\| \begin{matrix} a + ia' & a - ia' \\ b - ib' & b - ib' \end{matrix} \right\|,$$

et soit $(\xi + i\xi', \xi - i\xi')$ un point du module ϖ ayant T pour base. Pour avoir une représentation réelle associons à ϖ le module ϖ' (réseau de parallélogrammes) formé par les points $M'(\xi, \xi')$. La spanne $S(\text{OM}) = |\xi + i\xi'|$ est égale à la vraie distance OM'; son corps caractéristique étant convexe, les tableaux minima V sont aussi réduits. Pour les trouver, il nous faut donc chercher dans ϖ' les couples de points A'_1, A'_2, tels qu'aucun point de ϖ' ne soit plus rapproché de O que A'_1 et qu'aucun point, exception faite de ceux de la droite OA'_1, ne soit plus rapproché de O que A'_2. Si l'on remplace T par T × E

$$E = [\alpha + i\beta, \alpha - i\beta], \qquad \alpha + i\beta = \sqrt{\alpha^2 + \beta^2}(\cos\varphi + i\sin\varphi),$$

ceci a pour effet de multiplier l'imaginaire $\xi + i\xi'$ par l'imaginaire fixe $\alpha + i\beta$, c'est-à-dire revient à faire sur les points de ϖ' une même rotation d'angle φ suivie d'une homothétie de rapport $\sqrt{\alpha^2 + \beta^2}$. Cette opération ne change donc pas les rapports mutuels des distances OM', de sorte que les transformés des points A'_1, A'_2 jouissent de la même propriété dans le nouveau module. Donc les nouveaux réduits sont V × E et *l'ensemble des tableaux susceptibles de devenir réduits après une dilatation est identique à l'ensemble des tableaux réduits pour un* T *déterminé.*

Indiquons rapidement les divers cas qui peuvent se présenter dans la recherche de ces tableaux réduits : s'il n'y a qu'une indécision de signe pour A_1 et A_2, il y a quatre tableaux réduits,

$$V = \begin{Vmatrix} a_1 + ia'_1 & a_1 - ia'_1 \\ a_2 - ia'_2 & a_2 - ia'_2 \end{Vmatrix}, \qquad |-1, -1|V, \qquad |-1, 1|V, \qquad |1, -1|V.$$

S'il y a indécision pour le choix du deuxième point entre $\pm A_2$ et $\pm A_3$, un calcul simple donne la valeur de A_3 et montre que, en plus des tableaux réduits déjà obtenus, il en existe quatre autres, produits des premiers à gauche par l'un des tableaux

$$\begin{Vmatrix} 1 & 0 \\ \pm 1 & 1 \end{Vmatrix}.$$

Il peut y avoir encore indécision entre $\pm A_1$ et $\pm A_2$, si

$$S(OA_1) = S(OA_2);$$

alors, en plus des quatre premiers tableaux existent quatre nouveaux déduits des premiers par un changement de lignes, ou encore par une multiplication à gauche par

$$\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}.$$

Enfin, il peut y avoir combinaison des deux cas précédents, c'est-à-dire indécision entre $\pm A_1$, $\pm A_2$, $\pm(A_2 + A_1)$ ou $\pm(A_2 - A_1)$; les points de $\mathfrak{C}'$ ont alors dans le plan une disposition en *quinconce* ou encore forment un *pavage hexagonal*. On a dans ce cas vingt nouveaux tableaux obtenus en multipliant les premiers à gauche par l'un des deux systèmes de cinq tableaux

$$\begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ \pm 1 & 1 \end{Vmatrix}, \quad \begin{Vmatrix} \pm 1 & 1 \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} \pm 1 & 1 \\ 0 & 1 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & 1 \\ \pm 1 & 1 \end{Vmatrix}.$$

La forme décomposable associée à T est une forme binaire quadratique définie

$$F(x, y) = (ax + by)^2 + (a'x + b'y)^2,$$

les formes associées aux V, quel que soit le cas considéré, sont identiques seulement à deux formes distinctes,

$$\Phi(x, y) = Ax^2 \pm 2Bxy + Cy^2;$$

ces formes sont équivalentes à f, on peut donc les considérer comme *réduites*. *Elles vérifient d'ailleurs les conditions données par Gauss pour définir la forme réduite d'un système*

$$C \geq A \geq |2B|,$$

et pour l'une d'elles le coefficient du terme rectangle est positif. La première de ces conditions, qui peut s'écrire

$$a_1'^2 + a_1^2 \leq a_2'^2 + a_2^2,$$

exprime en effet que A_2 n'est pas plus rapproché de l'origine que A_1. La seconde peut s'écrire

$$a_1'^2 + a_1^2 \pm 2(a_1 a_2 + a_1' a_2') + a_2^2 + a_2'^2 \geq a_2^2 + a_2'^2,$$

et exprime que l'un des points $A_2 \pm A_1$ n'est pas plus rapproché que A_2. Les trois cas d'ambiguïté correspondent respectivement aux cas limites des conditions de Gauss

$$C > A = |2B|, \qquad C = A > |2B|, \qquad C = A = |2B|.$$

Il peut être intéressant de remarquer que la considération de la forme quadratique associée permet de classer les tableaux réduits V en deux ensembles, suivant que le coefficient du terme rectangle est positif ou négatif. On aurait pu arriver au même résultat en étudiant des classes (équivalence propre) au lieu de systèmes de tableaux.

Tableaux réels. — Passons maintenant au cas d'un tableau du deuxième ordre à termes réels,

$$T = \begin{Vmatrix} a & a' \\ b & b' \end{Vmatrix},$$

et soit (ξ, ξ') un point du module $\mathfrak{T}$ ayant T pour base. Supposons, pour simplifier, $\frac{a}{b}$ et $\frac{a'}{b'}$ irrationnels ; il n'y a qu'un seul tableau minimum vérifiant les conditions (1) (2) et (2 *bis*) ; il est donc réduit. En outre, il existe une infinité de points de $\mathfrak{T}$ vérifiant les inégalités (Chap. II, *Modules finis*),

$$\xi > M > 0, \qquad |\xi'| < \varepsilon.$$

Effectuons sur T la dilatation définie par

$$E = |\pm\lambda, \pm\lambda'|, \qquad (\lambda, \lambda') > 0 ;$$

elle remplace un point (ξ, ξ') par $(\pm\lambda\xi, \pm\lambda'\xi')$ et la spanne de l'origine au point (ξ, ξ') devient, puisqu'elle ne dépend que des valeurs absolues des coordonnées,

$$(3) \qquad f(\lambda\xi, \lambda'\xi') \qquad (\lambda, \lambda') > 0.$$

Donc, tout couple de points de $\mathfrak{T}$ susceptibles de devenir, après une dilatation convenable, un tableau réduit, constitue au signe près un tableau réduit équivalent à T lorsqu'on remplace la spanne par la spanne à deux paramètres, en donnant à ces paramètres des valeurs convenablement choisies. Réciproquement tous les tableaux réduits relativement à la fonction (3) où λ, λ' sont des paramètres arbitraires, sont susceptibles de devenir des tableaux réduits après une dilatation convenable. C'est le *principe de la réduction continuelle d'Hermite* [1] (ainsi appelé à cause de l'introduction des paramètres continus). Cherchons donc l'ensemble des tableaux réduits relativement à la fonction (3); à chaque système de valeurs λ, λ' ne correspond qu'un seul tableau réduit, mais la réciproque n'est pas vraie.

Remarquons d'abord qu'on obtient le même tableau réduit si l'on remplace λ, λ' par $t\lambda$, $t\lambda'$, car cette opération multiplie les spannes de tous les points [2] par t et ne change pas leurs rapports mutuels. On peut donc se borner à considérer les systèmes de paramètres dont le produit est égal à 1, ou encore au lieu de la fonction (3) la fonction

$$(3\ bis) \qquad f\left(\lambda\xi, \frac{1}{\lambda}\xi'\right) = S_\lambda(OM).$$

Ceci convenu, on peut montrer, comme nous l'indiquerons ultérieurement, qu'il existe une suite infinie dans les deux sens d'intervalles pavant $(0, \infty)$,

$$0 < \dots < \lambda_{-2} \leq \lambda_{-1} \leq \lambda_1 \leq \lambda_2 \leq \dots < +\infty \qquad \begin{pmatrix} \lim \lambda_i = +\infty \\ \lim \lambda_{-i} = 0 \end{pmatrix};$$

tels que dans chaque intervalle existe un seul tableau réduit. On obtient par le fait une suite de tableaux réduits ordonnée et illimitée dans les deux sens.

---

(1) Il employait toutefois pour f au lieu de la spanne la distance ordinaire.

(2) Ou encore, revient à faire sur $\mathfrak{T}$ une homothétie.

Mais on doit toujours à Hermite une méthode pour obtenir un ensemble plus simple de tableaux réduits, en considérant seulement certains tableaux particulièrement remarquables de l'ensemble précédent (Hermite appelait les formes correspondantes *réduites principales*); chacun d'eux est tel que, *pour une valeur convenable l_1 de λ, non seulement il est réduit, mais encore les points qui le constituent sont à une même spanne de l'origine* (*minima simultanés*). Avec l'hypothèse faite, ceci n'est possible que si ces spannes sont de rang différent.

Montrons l'existence de tels tableaux; soit un point $A(\alpha, \alpha')$ rendant f minimum pour une certaine valeur de λ, tout point (ξ, ξ') de $\mathfrak{C}$ à l'exception de $(-\alpha, -\alpha')$ et (o, o) vérifie au moins l'une des inégalités

$$|\xi| > |\alpha| \quad \text{ou} \quad |\xi'| > |\alpha'|;$$

sinon un certain point P aurait ses coordonnées inférieures (¹) en valeur absolue à celles de A et, quel que soit λ, la spanne de ce point à o serait inférieure à celle de A. Mais alors si l'on considère la valeur λ_1 du paramètre défini par

$$\lambda_1 |\alpha| = \frac{1}{\lambda_1} |\alpha'| = S_{\lambda_1}(\text{OA}),$$

tout point M de $\mathfrak{C}$ vérifie au moins l'une des inégalités

$$\lambda_1 |\xi| > S_{\lambda_1}(\text{OA}), \quad \text{ou} \quad \frac{1}{\lambda_1} |\xi'| > S_{\lambda_1}(\text{OA}),$$

donc

$$S(\text{OM}) > S(\text{OA}),$$

et $S(\text{OA})$ est minimum pour cette valeur λ_1; par raison de continuité, elle le sera encore pour des valeurs infiniment voisines. Ceci posé, faisons croître λ à partir de λ_1. $S(\text{OA})$ devient égal à $\lambda|\alpha|$, puisque $\frac{1}{\lambda}|\alpha'|$ décroît. Mais il ne peut rester indéfiniment minimum (²), car si l'on considère un point (δ, δ') de $\mathfrak{C}$ tel que $|\delta| < |\alpha|$ pour une valeur suffisamment grande de λ, la spanne

(¹) L'égalité est impossible par suite de l'irrationalité de $\frac{a}{b}$.

(²) Il n'en serait plus nécessairement ainsi si $\frac{a}{b}$ n'était pas irrationnel.

de ce point devient aussi égale à $\lambda|\xi|$, donc inférieure à celle de A. Donc, toujours pour raison de continuité, il existe une valeur l_1 de λ que nous appellerons *critique*, pour laquelle S(OA) cesse d'être minimum ([1]) en étant égal à la spanne d'un autre point B(β, β'), qui est de rang 2. Manifestement B n'est pas sur OA, il forme donc, avec A comme première ligne, un tableau à déterminant non nul V_1 répondant à la question. On voit en même temps que, pour des valeurs de λ supérieures à l_1, S(OA) n'est plus minimum; pour des valeurs inférieures à λ_1, S(OA) est de rang 2, de sorte qu'on a ainsi le seul tableau répondant à la question et dont A est première ligne. Si l'on fait croître λ à partir de l_1, S(OB) est minimum, d'abord de rang 2, puis change de rang pour une certaine valeur λ_2 et cède la place à un point C pour une valeur l_2; B et C forment un nouveau tableau V_2 répondant à la question pour cette valeur l_2, et ainsi de suite. De même, en faisant décroître λ à partir de λ_1, on aurait obtenu des valeurs l_{-1}, l_{-2}, ... et des tableaux V_{-1}, V_{-2}, ... Par ce cheminement, obtient-on tous les tableaux? Il n'en existe pas pour des valeurs intercalaires des λ, il suffit de montrer que les l_i deviennent infiniment grands et les l_{-i} infiniment petits, ou encore qu'il n'y a qu'un nombre fini de valeurs critiques dans tout intervalle I intérieur à $(0, \infty)$. Soient pour cela (e_1, e'_1), (e_2, e'_2) des points de $\mathfrak{G}$ tels que l'intervalle

$$\left(\sqrt{\left|\frac{e'_1}{e_1}\right|}, \sqrt{\left|\frac{e'_2}{e_2}\right|}\right)$$

comprenne I. Pour toute valeur de λ dans I,

$$f\left(\lambda e_1, \frac{1}{\lambda} e'_1\right) = \lambda|e_1|, \qquad f\left(\lambda e_2, \frac{1}{\lambda} e'_2\right) = \frac{1}{\lambda}|e'_2|.$$

Donc tout point M tel que S_λ(OM) soit minimum pour une valeur de λ comprise dans I doit vérifier

$$\begin{aligned} \lambda|\xi| &< \lambda|e_1| \\ \frac{1}{\lambda}|\xi'| &< \frac{1}{\lambda}|e'_2| \end{aligned} \qquad \text{ou} \qquad \begin{aligned} |\xi| &< |e_1|, \\ |\xi'| &< |e'_2|. \end{aligned}$$

([1]) On aurait pu présenter cette démonstration un peu différemment, de façon à n'avoir pas à se servir de raisons de continuité. Il m'a semblé préférable de conserver à peu près la marche suivie par Hermite; elle a au moins cet avantage de s'étendre plus aisément au cas général.

il ne peut y en avoir qu'un nombre fini et, par conséquent, un nombre fini de valeurs critiques [1].

La suite de tableaux, illimitée dans les deux sens

$$\ldots,\quad V_{-2},\quad V_{-1},\quad V_1,\quad V_2,\quad \ldots$$

est rangée dans le même ordre que les valeurs critiques sur la demi-droite $(0, \infty)$ ou que les logarithmes de ces valeurs sur la droite $(-\infty, +\infty)$. On a bien ainsi *un ensemble réduit* ; sa définition et son classement sont indépendants du tableau T qui définit le système ; d'autre part, si l'on remplace T par $T' = TE$,

$$E = [r, r'] \qquad (r > 0),$$

la suite

$$\ldots,\quad V_{-2}\times E,\quad V_{-1}\times E,\quad V_1\times E,\quad V_2\times E,\quad \ldots$$

vérifie les mêmes propriétés que la suite précédente, mais pour les valeurs $l_i \times \sqrt{\left|\frac{r'}{r}\right|}$ qui sont dans le même ordre de grandeur que les l_i. En outre, on n'a pu introduire de nouveaux tableaux, car on peut recommencer le même raisonnement pour T considéré comme égal à $T' \times E^{-1}$.

Nous avons supposé $r > 0$; dans le cas contraire, les tableaux de la nouvelle suite auraient les termes de leur première colonne négatifs, de sorte que pour avoir un ensemble réduit au sens strict du mot, il faudrait ajouter à la suite précédente les mêmes tableaux [2] multipliés par $[-1]$.

---

[1] En approfondissant un peu ce raisonnement, on verra sans difficulté que S(OA) est minimum pour l'intervalle (l_{-1}, l_1). Ceci permettrait de trouver les résultats indiqués précédemment pour la suite complète des tableaux réduits.

[2] Pour compléter la question il y aurait lieu de chercher des conditions nécessaires et suffisantes pour qu'un tableau T donné *a priori* appartienne à l'ensemble réduit du système qu'il définit, et aussi une méthode de calcul (qui se trouve identique à celle des fractions continues) pour trouver les termes de l'ensemble. Pour ces questions, de même que pour l'étude du cas où $\frac{a}{b}$ et $\frac{a'}{b'}$ ne seraient plus tous deux irrationnels, je renvoie à mon Mémoire déjà cité. J'ajouterai une dernière remarque : au lieu d'employer la spanne on aurait pu utiliser une autre distance généralisée et, en particulier, comme l'a fait Hermite, la distance ordinaire. On obtient les mêmes ensembles, à des exceptions isolées près.

Réduction continuelle pour le $n^{\text{ième}}$ ordre.

Nous pouvons maintenant, en procédant par induction, traiter le cas de tableaux du $n^{\text{ième}}$ ordre (définis à une dilatation près) à r colonnes réelles et $2s$ imaginaires conjuguées. Supposons encore qu'il n'y ait aucune relation linéaire, homogène à coefficients entiers entre les termes d'une même colonne de T et appelons $\mathfrak{T}$ le module ayant T pour base. En induisant le cas du second ordre imaginaire, on est amené à penser que seules importent les valeurs absolues des coordonnées des points M de $\mathfrak{T}$. Nous désignerons ces $r + s = p$ valeurs absolues par

$$|\delta_1|, \quad |\delta_2|, \quad \ldots, \quad |\delta_p|,$$

ou encore par $|\theta_i|$, et nous utiliserons aussi la spanne à p paramètres, généralisation de la fonction (3),

$$(4) \qquad S_\lambda(\text{OM}) = \text{maximum}(\lambda_1|\delta_1|, \lambda_2|\delta_2|, \ldots, \lambda_p|\delta_p|);$$

le rang de cette spanne sera le rang du ou des $\lambda|\delta|$ maxima. Quand il nous arrivera de distinguer les n coordonnées $(x_1, x_2, \ldots, x_n)$ d'un point de $\mathfrak{T}$, nous appellerons $t_1, t_2, \ldots, t_n$ les valeurs des paramètres λ qui multiplient les valeurs absolues des coordonnées correspondantes; à deux coordonnées imaginaires conjuguées correspondront des t égaux.

Ceci posé, on peut, comme dans le cas du deuxième ordre à termes réels, montrer que :

Il existe une infinité de systèmes de valeurs des paramètres, définis chacun à un facteur près de proportionnalité, tels que pour chacun d'eux existent $r+s$ points de $\mathfrak{T}$ dont les spannes soient égales, de rang différent et au plus égales aux spannes des autres points de $\mathfrak{T}$.

Partons d'un système déterminé de paramètres; pour ce système, on peut trouver au moins un point A tel que S(OA) soit minimum. Supposons plus généralement qu'il existe k points ($k \geqq 1$), A_1, $A_2, \ldots, A_k$ vérifiant les conditions de l'énoncé. En changeant s'il y a lieu l'ordre des δ, on peut supposer que les spannes $S(OA_i)$

sont respectivement de rang 1, 2, ..., k.

$$S(OA_1) = l_1|\theta_1^1|, \quad S(OA_2) = l_2|\theta_2^2|, \quad \ldots, \quad S(OA_k) = l_k|\theta_k^k|,$$
$$S(OA_1) = S(OA_2) = \ldots = S(OA_k) = m,$$

le système de paramètres étant

$$l_1, \quad \ldots, \quad l_k, \quad l_{k+1}, \quad \ldots, \quad l_p.$$

Remplaçons dans le système l_{k+1} par λ_{k+1} et faisons décroître λ_{k+1} d'une façon continue depuis la valeur l'_{k+1}. Les k spannes précédentes restent égales à m, mais ne resteront pas indéfiniment minima. Soit, en effet, un point B de $\mathcal{E}$ dont les valeurs absolues des coordonnées vérifient les $p-1$ inégalités

$$l_i|\xi_i| < m \qquad [i = (1, 2, \ldots, p), \; k+1 \text{ excepté}];$$

d'après l'hypothèse, il y a une infinité de tels points B. Pour λ_{k+1} suffisamment petit, on a aussi

$$\lambda_{k+1}|\xi_{k+1}| < m \qquad \text{et} \qquad S(OB) < m.$$

Donc, par raison de continuité, il existe une valeur l_{k+1} de λ_{k+1}, pour laquelle m cesse d'être un minimum en étant égal à la spanne d'au moins un autre point $S(OA_{k+1})$. Mais, quel que soit ce point, cette spanne est de rang $k+1$; en effet, dans la variation, les spannes de rang différent de $k+1$, qui étaient primitivement supérieures à m, restent toujours supérieures. Le raisonnement est valable pour k quelconque, on peut donc le recommencer à partir du système de paramètres

$$l_1, \quad l_2, \quad \ldots, \quad l_{k+1}, \quad l_{k+2}, \quad \ldots, \quad l_p,$$

et montrer l'existence d'un point A_{k+2} et d'un paramètre l_{k+2}. Et ainsi de suite jusqu'à obtenir p points et un système de paramètres correspondants.

Si l'on remplace ces p paramètres par p autres proportionnels (mais positifs), on multiplie les spannes par un même facteur et l'on ne change pas leurs rapports mutuels, il leur correspond donc les mêmes points A_i jouissant des mêmes propriétés.

Un tel système de paramètres sera dit *un système critique* et les *p points correspondants des minima simultanés*. Pour déterminer complètement les systèmes critiques nous conviendrons de

poser

$$(4\ bis)\qquad \begin{cases} t_1 t_2 \ldots t_n = 1 \\ \text{ou} \\ (\lambda_1)^{u_1}(\lambda_2)^{u_2}\ldots(\lambda_p)^{u_p} = 1 \qquad (u_i = 1 \text{ ou } 2). \end{cases}$$

Alors à p minima simultanés correspond un seul système critique défini par l'équation précédente et

$$\lambda_1|\theta_1^1| = \lambda_2|\theta_2^2| = \ldots = \lambda_p|\theta_p^p|.$$

Mais réciproquement à chaque système critique peut correspondre *plusieurs systèmes de minima, toutefois en nombre fini*. On les obtiendra tous en remplaçant chacun des points A_k successivement par chacun des points A'_k de $\mathfrak{C}$ tels que $S(OA'_k)$ soit égal à $S(OA_k)$ et de même rang. On obtient déjà ainsi les 2^p systèmes

$$\pm A_1, \quad \pm A_2, \quad \ldots, \quad \pm A_p,$$

mais on peut aussi en avoir d'autres, si certaines des coordonnées sont imaginaires (nous en avons eu des exemples dans le cas du deuxième ordre imaginaire).

Pour montrer qu'il existe une infinité de systèmes critiques nous emploierons la représentation géométrique suivante : à tout système de nombres positifs λ_k vérifiant la condition (4 *bis*), nous ferons correspondre le point d'un espace à p dimensions

$$(\rho_1, \rho_2, \ldots, \rho_p), \qquad \rho_i = \log\lambda_i.$$

Tous ces points forment, si $p > 1$, un sous-espace Λ de dimension $p - 1$ et d'équation

$$(4\ ter)\qquad u_1\rho_1 + u_2\rho_2 + \ldots + u_p\rho_p = 0.$$

Alors tout point A d'un tableau réduit est tel que $S(OA)$ est minimum pour un point de Λ; considérons tous les points de Λ pour lesquels $S(OA)$ reste minimum. On pouvait vérifier sans peine que cet ensemble est *un domaine d'un seul tenant* [1] *sans trous*, et que *sa frontière est composée de portions de sous-espaces à $p - 2$ dimensions*, il nous suffira de démontrer qu'il est borné.

---

[1] Chacun de ces domaines se décompose en p domaines partiels à l'intérieur desquels la spanne a un rang déterminé. Nous avons eu un exemple de tels domaines sur une droite (deuxième ordre). Pour un exemple dans le plan, *voir* le Mémoire cité.

Pour cela, considérons p points de $\mathfrak{C}$, le $k^{\text{ième}}$ B_k étant tel que les valeurs absolues de ses coordonnées, sauf la $k^{\text{ième}}$, soient inférieures aux valeurs absolues des coordonnées correspondantes de A. Mais alors pour que S(OA) soit inférieur à S(OB$_1$), il faut que cette dernière spanne soit de rang 1, c'est-à-dire que

$$\lambda_1|\delta_1^1| > \lambda_2|\delta_2^1|, \quad \lambda_1|\delta_1^1| > \lambda_3|\delta_3^1|, \quad \ldots, \quad \lambda_1|\delta_1^1| > \lambda_p|\delta_p^1|$$

et de même pour B$_2$, B$_3$, ... Ces p systèmes d'inégalités fournissent des limites supérieures et inférieures, par exemple, pour les rapports $\frac{t_i}{t_j}$, ce qui, en ayant égard à (4 *bis*), montre bien que l'ensemble correspondant dans A est borné. D'autre part, ces divers domaines qui peuvent avoir des points communs doivent couvrir (¹) tout le sous-espace A puisqu'à tout système de paramètres correspond au moins un minimum. Donc, si $p > 1$, il y a une infinité d'ensembles, donc de minima, donc de systèmes de minima simultanés (de chaque minimum on peut déduire un tel système).

Utilisons encore cette représentation géométrique pour montrer que les systèmes critiques sont isolés (*leur ensemble n'a pas de point limite*). Il suffit de montrer que dans tout domaine I *borné* de A n'existe qu'un nombre fini de points critiques. Nous y arriverons en suivant une marche analogue à celle du deuxième ordre. Déterminons un point D$_1$ tel que, pour tout système de paramètres contenus dans I, la spanne S(OD$_1$) soit de rang 1, il suffit pour cela de prendre $|\delta_2|$, ..., $|\delta_p|$ suffisamment petits; déterminons de même D$_2$, ..., D$_p$ tels que, dans I,

$$S(OD_1) = \lambda_1|\delta_1^1|, \quad S(OD_2) = \lambda_2|\delta_2^2|, \quad \ldots, \quad S(OD_p) = \lambda_p|\delta_p^p|.$$

Mais alors pour que la spanne d'un point de $\mathfrak{C}$ soit minimum pour un système de paramètres dans I, il faut que

$$|\delta_1| < |\delta_1^1|, \quad |\delta_2| < |\delta_2^2|, \quad \ldots, \quad |\delta_p| < |\delta_p^p|$$

et il n'y a qu'un nombre fini de tels points.

Ensemble réduit. — Les p minima simultanés forment une matrice de type (p, n) mais dont on ne peut affirmer qu'elle soit

---

(¹) Les systèmes critiques sont des points communs à p de ces ensembles.

de rang p, de sorte qu'en supposant même $s = 0$ et $p = n$, on n'est pas certain en général qu'une telle matrice constitue un tableau du module. On peut tourner la difficulté en considérant la spanne à p paramètres (4); on y remplace les paramètres par chaque système de valeurs critiques, et pour chaque distance généralisée ainsi obtenue on cherche le ou les tableaux minima (*conditions* 1, 2 *et* 2 *bis*) et les tableaux réduits correspondants; les premiers tableaux contiendront d'ailleurs plusieurs des minima simultanés (exactement k si l'on peut en trouver k et pas plus formant une matrice de rang k). L'ensemble ainsi obtenu se trouve ordonné; à chaque point critique de Λ correspond un nombre fini de tableaux de l'ensemble; les points ayant une disposition déterminée on peut considérer que cette disposition constitue un classement de ces tableaux.

Cet ensemble est bien réduit; étant défini à partir du module $\mathfrak{T}$, il est indépendant de la base choisie. D'autre part, si l'on remplace T par $T' = TE$, on remplace les valeurs absolues $|\partial_i|$ par $r_i|\partial_i|$, les r étant les valeurs absolues des termes de E. Donc, au lieu de faire les opérations sur le nouveau module $\mathfrak{T}'$, on peut les faire sur l'ancien en prenant pour spanne à p paramètres, la fonction

$$\text{maximum}(\lambda_1 r_1 |\partial_1|, \ldots, \lambda_p r_p |\partial_p|),$$

on obtient les mêmes systèmes de minima simultanés (à la dilatation près) et les mêmes tableaux réduits. Seuls les systèmes critiques sont changés et remplacés par

$$\frac{r_i l_i}{\sqrt[n]{r_1^{n_1} r_2^{n_2} \ldots r_p^{n_p}}} = \frac{r_i l_i}{\sqrt[n]{|\Delta(E)|}}.$$

La disposition des points critiques correspondants dans le sous-espace n'étant pas changée de ce fait, on peut dire que le classement de l'ensemble réduit est encore le même. Il y a la même restriction de signe à faire que pour le cas du deuxième ordre si la première colonne est réelle.

Les deux théorèmes de Minkowski.

Pour compléter la méthode précédente de réduction, il serait bon d'avoir des conditions nécessaires et suffisantes qui per-

mettent de reconnaître *a priori* si un tableau donné est réduit dans le système auquel il appartient (par exemple pour le deuxième problème cité au début de ce Chapitre). On peut trouver des conditions assez simples dans le cas du deuxième ordre, un peu plus compliquées pour le troisième ordre réel, il semble qu'il y aurait de grosses difficultés à aborder cette question dans le cas général. A son défaut, deux théorèmes énoncés par M. Minkowski permettent d'indiquer des *conditions nécessaires de réduction* qui nous suffiront au moins pour l'application aux nombres algébriques. Hermite était arrivé à de telles conditions en se servant de propriétés des formes quadratiques (distance ordinaire) qu'il utilisait dans sa méthode de réduction. Quoique nous ayons seulement utilisé la spanne, nous établirons les théorèmes [1] pour une distance généralisée quelconque vérifiant les conditions (5) du Chapitre I.

THÉORÈME I. — *Étant donné un module type de dimension* n, *de base* T *et formé par les points* A$(a_1, a_2, \ldots, a_n)$, *on a*

$$(5)\qquad |\text{minimum}\, f(a_1, a_2, \ldots, a_n)|^n \leqq \frac{2^n|\Delta(\mathrm{T})|}{\mathrm{J}},$$

J *étant une constante qui ne dépend que de la fonction* f.

Remarquons que la distance généralisée de deux points du module S(AA′) est égale à la distance de o au point A — A′, le minimum de f que nous appellerons m peut donc être considéré comme le minimum des distances S(AA′); ou encore : S(AA′) $< m$ est impossible sauf si A est confondu avec A′. Considérons les corps $\Gamma_{\frac{m}{2}}(\mathrm{A})$ définis par

$$\mathrm{S}(\mathrm{AM}) \leqq \frac{m}{2},$$

ces corps ainsi attachés à chaque point du module *n'empiètent pas*, c'est-à-dire qu'un point M ne peut être à la fois intérieur au sens étroit, à deux corps distincts $\Gamma_{\frac{m}{2}}(\mathrm{A})$ et $\Gamma_{\frac{m}{2}}(\mathrm{A}')$. Car les inégalités

$$\mathrm{S}(\mathrm{AM}) < \frac{m}{2}, \qquad \mathrm{S}(\mathrm{A}'\mathrm{M}) < \frac{m}{2}$$

(1) La démonstration ne serait pas simplifiée par la considération d'un cas particulier.

entraîneraient

$$S(AA') \leq S(AM) + S(A'M) < m,$$

ce qui exigerait que A et A' soient confondus (¹). Considérons alors tous les points E du module qui, par rapport à T, ont pour coordonnées relatives des nombres entiers e_i, au plus égaux, en valeur absolue, à un entier donné ω; il y a $(2\omega + 1)^n$ pareils points; appelons Ω le domaine formé par les corps Γ attachés à chacun de ces points. Le volume de ce domaine est égal, puisque les corps n'empiètent pas, à $(2\omega + 1)^n$ fois le volume de l'un d'eux qui est $\left(\frac{m}{2}\right)^n$ J, J étant le volume du corps caractéristique $\Gamma_1(o)$.

Ceci posé, cherchons à constituer un domaine qui contienne Ω et dont on puisse déterminer le volume. Appelons y_i les coordonnées relatives par rapport à T et soit ε une limite supérieure des $|y_i|$ pour les points de $\Gamma_1(o)$. Tout point de Ω vérifie alors l'un des systèmes d'égalités

$$(|y_1 - e_1|, |y_2 - e_2|, \ldots, |y_n - e_n|) \leq \varepsilon,$$

donc, *a fortiori*,

$$(|y_1|, |y_2|, \ldots, |y_n|) \leq \omega + \varepsilon.$$

Mais ces dernières égalités définissent un domaine limité (corps caractéristique d'une spanne) qui contient Ω. Le volume de ce nouveau domaine est

$$\begin{aligned} \int \cdots \int dx_1\, dx_2 \ldots dx_n &= |\Delta(T)| \int \cdots \int dy_1\, dy_2 \ldots dy_n \\ &= |\Delta(T)| \int_{-\omega-\varepsilon}^{\omega+\varepsilon} dy_1 \int_{-\omega-\varepsilon}^{\omega+\varepsilon} dy_2 \ldots \int_{-\omega-\varepsilon}^{\omega+\varepsilon} dy_n \\ &= |\Delta(T)|(2\omega + 2\varepsilon)^n. \end{aligned}$$

Ce volume devant être supérieur ou égal à celui de Ω, on a

$$(2\omega + 1)^n \left(\frac{m}{2}\right)^n J \leq |\Delta(T)|(2\omega + 2\varepsilon)^n,$$

ou

$$m^n \leq \frac{2^n |\Delta(T)|}{J} \left(\frac{2\omega + 2\varepsilon}{2\omega + 1}\right)^n;$$

(¹) Il peut y avoir des points communs aux frontières, car $S(AA') = m$ a des solutions.

cette inégalité ayant lieu quel que soit ω a encore lieu en remplaçant le deuxième membre par sa limite pour $\omega = \infty$ et c'est alors ce qu'il fallait démontrer ([1]).

Il peut arriver que la limite supérieure ainsi donnée pour le minimum de f soit effectivement atteinte, le raisonnement précédent précisé montre qu'il est pour cela nécessaire et suffisant que les corps Γ couvrent tout l'espace. Mais par contre, il peut aussi arriver que la limite supérieure soit beaucoup trop grande, ce qui se produit si les corps Γ laissent entre eux des intervalles assez grands (en volume). On peut indiquer une précision du théorème en considérant les tableaux minima.

Théorème II. — *Si dans un module type de base* T (*tableau d'ordre* n) *on considère un système de distances minima* (*conditions* 1),

$$S(OA_1) = m_1, \qquad S(OA_2) = m_2, \qquad \ldots, \qquad S(OA_n) = m_n,$$

on a

$$(5\ bis) \qquad m_1 m_2 \ldots m_n \leq \frac{2^n \Delta(T)}{J}.$$

Le deuxième membre de cette inégalité est le même que dans le théorème précédent qui est par suite une conséquence du nouveau ([2]), car m est égal à m_1 et m_1^n est au plus égal au premier membre de (5 *bis*).

Pour démontrer ce théorème, prenons pour base du module le tableau réduit U déduit du tableau minimum V comme il a été dit plus haut. Nous considérerons les différents corps

$$\Gamma_{\frac{m_1}{2}}(E), \quad \Gamma_{\frac{m_2}{2}}(E), \quad \ldots, \quad \Gamma_{\frac{m_n}{2}}(E)$$

([1]) En supposant, par exemple, $T = [1]$, c'est-à-dire en prenant pour module l'ensemble $\mathcal{C}$ des points de coordonnées entières, on peut énoncer cette conséquence assez curieuse du théorème :

Si un corps convexe ayant pour centre l'origine a un volume au moins égal à 2^n, *il contient, au sens large, au moins deux points à coordonnées entières, symétriques par rapport à l'origine.*

([2]) Il m'a paru cependant utile de donner une démonstration directe du premier théorème, d'une part, pour alléger un peu la démonstration du deuxième; d'autre part, parce que ce théorème a lui-même une grande importance et peut dans beaucoup de cas remplacer le deuxième.

que nous appellerons pour abréger $\Gamma^1(\text{E})$, $\Gamma^2(\text{E})$, ..., $\Gamma^n(\text{E})$; les points E sont les mêmes que précédemment (coordonnées relatives au plus égales à ω). A part les premiers, on ne peut plus affirmer qu'ils n'empiètent pas, on est même sûr du contraire si $m_2 > m_1$. Quoi qu'il en soit les points intérieurs à ces corps constituent respectivement des domaines limités $\Omega_1, \Omega_2, \ldots, \Omega_n$, dont les volumes $v_1, v_2, \ldots, v_n$ sont bien définis (1). Nous avons vu que

$$v_1 = (2\omega + 1)^n \left(\frac{m_1}{2}\right)^n J;$$

on peut encore affirmer en raisonnant comme précédemment que

$$v_n \leqq |\Delta(U)|(2\omega + 2\varepsilon')^n, \qquad \varepsilon' = \frac{m_n}{m_1}\varepsilon.$$

Nous allons alors établir des inégalités pour les rapports de deux v consécutifs. Nous pouvons pour cela faire un changement de coordonnées, car il a pour effet de multiplier ces volumes v par une même quantité (déterminant du tableau), et par suite, ne change pas leurs rapports mutuels. Dans ce qui va suivre nous supposerons l'espace rapporté au tableau réduit U, nous appellerons encore x_1, $x_2, \ldots, x_n$ les coordonnées relatives d'un point quelconque et v les volumes des domaines Ω_i. Le sous-espace défini par les k premières lignes de U est le même que celui défini par les k premières lignes de V, de sorte que la condition pour un point de n'être pas dans $\text{OA}_1\text{A}_2\ldots\text{A}_k$ peut s'exprimer en disant que les $n-k$ dernières coordonnées ne sont pas nulles simultanément. On déduit alors des conditions (1) qu'on ne peut avoir

$$S(\text{OA}) < m_k$$

que si les $n-k+1$ dernières coordonnées de A sont nulles, cette condition nécessaire n'étant pas, bien entendu, suffisante; en raisonnant comme pour le premier théorème, on voit que deux corps $\Gamma^k(\text{A})$, $\Gamma^k(\text{A}')$, ne peuvent empiéter que si les $n-k+1$ dernières coordonnées de A et A' sont les mêmes.

Répartissons les corps de Ω_k en $(2\omega+1)^{n-k+1}$ groupes de $(2\omega+1)^{k-1}$ corps, dans chaque groupe les centres des corps ayant

---

(1) On ne compte, bien entendu, qu'une fois les parties communes à deux ou plusieurs corps qui empiètent.

les mêmes $n - k + 1$ dernières coordonnées (nombres entiers). D'après ce qui précède, deux groupes distincts ne peuvent avoir de points communs de sorte que v_k est égal à la somme des volumes de chacun des groupes. Mais ces volumes sont égaux entre eux, car on peut établir entre les points de deux groupes une correspondance biunivoque qui consiste à ajouter aux $n - k + 1$ dernières coordonnées des constantes entières. On a donc

$$v_k = (2\omega + 1)^{n-k+1} w_k$$

$$\left\{ \begin{array}{c} w_k = \int \ldots \int dx_1\, dx_2 \ldots dx_n \\ f(x_1 - e_1, \ldots, x_{k-1} - e_{k-1}, x_k, \ldots, x_n) \leq \frac{1}{2} m_k, \end{array} \right.$$

$$|e_i| \text{ entier} \leq \omega.$$

Mais on peut calculer l'intégrale précédente en deux étapes,

$$(6) \qquad \left\{ \begin{array}{c} S = \int \ldots \int dx_1 \ldots dx_{k-1} \\ f(x_1 - e_1, \ldots, x_{k-1} - e_{k-1}, t_k, \ldots, t_n) \leq \frac{1}{2} m_k. \end{array} \right.$$

$$w_k = \int \ldots \int S\, dt_k \ldots dt_n.$$

Dans la deuxième intégrale les limites des t sont données par la condition que S existe ou encore que l'équation

$$(7) \qquad f(y_1, y_2, \ldots, y_{k-1}, t_k, \ldots, t_n) \leq \frac{1}{2} m_k,$$

ait des solutions en y.

Considérons maintenant le domaine Ω_{k-1}, si nous répartissons encore les corps en $(2\omega + 1)^{n-k+1}$ groupes, les centres des corps d'un même groupe ayant les mêmes $n - k + 1$ dernières coordonnées, *a fortiori* deux groupes n'empiètent pas et le volume est donné par

$$v_{k-1} = (2\omega + 1)^{n-k+1} w'_k.$$

$$w'_k = \int \ldots \int S_1\, dt'_k \ldots dt'_n.$$

$$\left\{ \begin{array}{c} S_1 = \int \ldots \int dx'_1 \ldots dx'_{k-1} \\ f(x'_1 - e_1, \ldots, x'_{k-1} - e_{k-1}, t'_k, \ldots, t'_n) \leq \frac{1}{2} m_{k-1}, \end{array} \right.$$

la limitation des t' étant donnée comme précédemment en remplaçant m_k par m_{k-1}. Pour comparer ce volume au précédent, multiplions les deux membres de la dernière condition par $\theta = \frac{m_k}{m_{k-1}}$, en faisant porter cette multiplication sur chaque variable dans f [deuxième condition (5)] et faisons (¹) le changement de variable $\theta t'_i = t_i$, on obtient

$$\omega'_k = \left(\frac{1}{\theta}\right)^{n-k+1} \int \cdots \int S_1 \, dt_k \ldots dt_n,$$

$$(6\,bis) \qquad \left\{ \begin{aligned} & S_1 = \int\int dx'_1 \ldots dx'_{k-1}, \\ & f[\ldots, \theta(x'_{k-1} - e_{k-1}), t_k, \ldots] \leqq \frac{1}{2} m_k. \end{aligned} \right.$$

La limitation des t est cette fois la même que pour l'évaluation de S. Donc pour comparer ω_k et ω_{k-1}, il suffit de comparer S et S_1 pour un même système de valeurs de $t_k, \ldots, t_n$. Un tel système étant choisi, les équations (6) et (6 *bis*) définissent des domaines dans le sous-espace de dimension $k-1$, défini par $n-k-1$ équations $x_i = t_i$. On ne peut pas en général affirmer que le domaine (6) soit inclus dans le domaine (6 *bis*), mais on peut, en translatant l'un des deux domaines, s'arranger pour qu'il en soit ainsi. Soit $(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$ une solution de (7) et faisons dans l'intégrale S le changement de variables (translation),

$$x_i = x'_i + \frac{\theta - 1}{\theta} \alpha_i,$$

on obtient

$$S = \int \cdots \int dx'_1 \ldots dx'_{k-1}$$

pour

$$(6\,ter) \qquad f\left[\ldots, \theta(x_i - e_i) + \frac{\theta - 1}{\theta} \alpha_i, \ldots, t_j, \ldots\right] \leqq \frac{1}{2} m_k.$$

Mais tout point du domaine (6 *bis*) est intérieur à (6 *ter*). En effet

(¹) Dans le cas $n = 3$ (coordonnées x, y, z) et $k = 3$, on peut exprimer ce changement en disant qu'on fait une dilatation de cote sur les corps de Ω_2 dont les centres sont dans le plan xoy. La cote de ces nouveaux corps varie alors dans les mêmes limites que pour les corps de Ω_3 ayant leurs centres dans xoy. Les surfaces S et S_1 sont celles des sections de ces deux groupes de corps par un même plan parallèle à xoy. On interprétera sans difficulté les opérations faites pour leur comparaison.

la condition (6 *bis*) exprime que le point $[\dots, \theta(x'_i - e_i), \dots, t_j, \dots]$ est intérieur au sens large au corps $\Gamma^k(\omega)$, il en est de même du point $(\dots, \alpha_i, \dots, t_j, \dots)$, donc aussi du point

$$\left(\dots, \frac{\theta(x'_i - e_i) + (\theta - 1)\alpha_i}{1 + (\theta - 1)}, \dots, t_j, \dots\right)$$
$$= \left(\dots, x'_i - e_i + \frac{\theta - 1}{\theta}\alpha_i, \dots, t_j, \dots\right)$$

qui appartient au segment déterminé par les deux premiers, puisque $\theta > 1$. Donc S_1 est au plus égal (¹) à S, quels que soient les t et en passant de là aux volumes v,

$$\theta^{n-k+1} v_k \leqq v_{k-1}$$

ou

$$\frac{v_k}{v_{k-1}} \geqq \left(\frac{m_k}{m_{k-1}}\right)^{n-k+1}.$$

Ceci est vrai quel que soit k qui peut prendre les valeurs 2, 3, ..., n; en multipliant ces $n - 1$ inégalités membre à membre, on obtient

$$\frac{v_n}{v_1} \geqq \frac{m_2 m_3 \dots m_n}{(m_1)^{n-1}}$$

ou, en ayant égard à la valeur de v_1 et à l'inégalité obtenue pour v_n,

$$m_1 m_2 \dots m_n \leqq \frac{2^n\,|\Delta(U)|}{J} \left(\frac{2\omega - 2\varepsilon}{2\omega - 1}\right)^n;$$

en remplaçant le deuxième membre par sa limite pour ω infini, on trouve (5 *bis*).

Évaluons par exemple la valeur du deuxième membre de (5) ou (5 *bis*) en prenant pour f *la spanne à p paramètres* (4). Supposons l'espace semi-réel $(x_1, \dots, x_r, y_1 \pm iy'_1, \dots, y_s \pm iy'_s)$,

$$\left\{\begin{array}{l} J = 2^s \int \dots \int dx_1\, dx_2 \dots dx_r\, dy_1\, dy'_1 \dots dy_s\, dy'_s \\ \qquad \lambda_i |x_i| < 1, \qquad\qquad \mu_j^2 (y_j^2 - y_j'^2) < 1. \end{array}\right.$$

l'intégrale est un produit de $r + s$ intégrales faciles à calculer

(¹) Il y a sûrement égalité si $\theta = 1$; d'ailleurs dans ce cas, on a identité entre Ω_{k1}, Ω_{k-1}. Mais il pourrait aussi y avoir égalité dans d'autres cas.

(longueur d'un segment ou surface d'un cercle)

$$J = 2^s \frac{2^r}{\lambda_1 \ldots \lambda_r} \frac{\pi^s}{\mu_1^2 \ldots \mu_s^2},$$

et le deuxième membre des inégalités est

$$\frac{2^s}{\pi^s} |\Delta(T)| \lambda_1 \ldots \lambda_n \mu_1^2 \ldots \mu_s^2 = \frac{2^s}{\pi^s} |\Delta(T)| t_1 t_2 \ldots t_n.$$

Du premier théorème de Minkowski on peut déduire un résultat intéressant, trouvé auparavant par Hermite, sur l'approximation simultanée d'irrationnelles par des fractions de même dénominateur. Soient par exemple trois nombres irrationnels a, b, c et le module $\mathfrak{C}$ ayant pour base

$$A = \begin{Vmatrix} a & b & c & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix};$$

considérons la spanne

$$S_\lambda(OA) = \text{maximum}\left(\lambda|\alpha|, \lambda|\beta|, \lambda|\gamma|, \frac{1}{\lambda^3}\delta\right),$$

α, β, γ, δ étant les coordonnées d'un point du module. Le minimum de cette distance est au plus égal à $|\Delta(A)| = 1$, ce qu'on peut encore énoncer : étant donné λ, il existe quatre nombres entiers x, y, z, t tels qu'on ait simultanément

$$\lambda|xa + y| \leq 1, \qquad \lambda|xb + z| \leq 1, \qquad \lambda|xc + t| \leq 1, \qquad \frac{1}{\lambda^3}|x| \leq 1,$$

ou encore on peut trouver une infinité de valeurs x, y, z, t, telles que

$$\left|a + \frac{y}{x}\right| \leq \frac{1}{|x|^{\frac{4}{3}}}, \qquad \left|b + \frac{z}{x}\right| \leq \frac{1}{|x|^{\frac{4}{3}}}, \qquad \left|c + \frac{t}{x}\right| \leq \frac{1}{|x|^{\frac{4}{3}}}.$$

Les résultats que nous avons obtenus s'appliquent évidemment aux tableaux de l'ensemble réduit. Soit un système de paramètres critiques et l'un des tableaux minima V correspondant à ces valeurs. Un terme σ du développement du déterminant $\Delta(V)$ est le produit de coordonnées de rangs différents appartenant respectivement aux points de V. Alors si dans l'expression de σ nous

multiplions chaque coordonnée par le paramètre critique t de même rang, on obtient un produit, égal au précédent, de n nouveaux facteurs, chacun d'eux étant au plus égal en valeur absolue à

$$S(OA_1) = m_1, \qquad S(OA_2) = m_2, \qquad \dots, \qquad S(OA_n) = m_n.$$

Donc

$$|\tau| \le m_1 m_2 \dots m_n \le \left(\frac{2}{\pi}\right)^s |\Delta(T)|.$$

Chaque terme du développement de $\Delta(V)$ est ainsi limité en valeur absolue, en fonction seulement de $\Delta(T)$; il en est de même de $\Delta(V)$ qui, étant une somme de $n!$ termes τ, est au plus égal à

$$n!\, H\, |\Delta(T)|, \qquad \left[H = \left(\frac{2}{\pi}\right)^s\right].$$

Soit maintenant $U = SV$ le tableau réduit déduit de V; on a

$$|\Delta(S)| = \left|\frac{\Delta(U)}{\Delta(V)}\right| = \left|\frac{\Delta(T)}{\Delta(V)}\right| \ge \frac{1}{H\, n!};$$

or, S est un tableau à termes fractionnaires au plus égaux à 1, en valeur absolue. L'inégalité précédente montre que les dénominateurs et numérateurs de ces termes sont limités supérieurement quel que soit le module considéré et seulement en fonction de r et de s.



CHAPITRE VII.

RÉDUCTION D'UNE BASE D'UN CORPS ALGÉBRIQUE.

Considérons maintenant un tableau de base d'un corps algébrique K,

$$T = \left\| \begin{matrix} \omega_1'^1 & \omega_2'^1 & \dots & \omega_n'^1 \\ \omega_1'^2 & \omega_2'^2 & \dots & \omega_n'^2 \\ \dots & \dots & \dots & \dots \\ \omega_1'^n & \omega_2'^n & \dots & \omega_n'^n \end{matrix} \right\|.$$

les $\omega^{(i)}$ sont des nombres algébriques de K, le déterminant $\Delta(T)$ est différent de o, r colonnes sont réelles et $2s$ imaginaires conjuguées. Il n'existe aucune relation à coefficients entiers entre les termes d'une colonne de T, car la même relation devrait exister entre les termes des autres colonnes et $\Delta(T)$ serait nul. Nous pouvons donc appliquer au système de tableaux équivalents à T la méthode de réduction continuelle. Supposons, en faisant s'il y a lieu une dilatation, que T est composé d'entiers algébriques ; tout point du module $\mathfrak{E}$ de base T a pour coordonnées les n conjugués d'un entier complexe de K (la réciproque n'est vraie que si T est une base des entiers du corps); nous sommes alors en mesure de préciser les inégalités obtenues pour les tableaux réduits.

Soit encore V un tableau minimum formé des n points

$$A_i \qquad (\alpha_1'^{i}, \alpha_2'^{(i)}, \dots, \alpha_n'^{i}),$$

correspondant au système de paramètres critiques $t_1, t_2, \dots, t_n$ dont le produit est 1. Les inégalités

$$t_j | \alpha_j'^i | \leqq m_i$$

entraînent

$$| N(\alpha^{i}) | = | \alpha_1'^i \alpha_2'^i \dots \alpha_n'^i | \leqq (m_i)^n.$$

Mais d'autre part, les $\alpha^{(i)}$ étant des entiers complexes, leur norme est

au moins égale à 1 et il en est de même de chaque minimum m_i, de sorte que dans l'inégalité (5 *bis*) de Minkowski chacun des facteurs du premier membre est inférieur au second membre

$$m_i \leq H|\Delta(T)|.$$

Donc si l'on fait sur V la dilatation de déterminant 1,

$$V \times [t_1, t_2, \ldots, t_n],$$

chaque terme de ce tableau (et non plus seulement chaque terme du développement du déterminant), est limité supérieurement en valeur absolue [inférieur à $H|\Delta(T)|$]. Il en est de même des termes du tableau réduit [1],

$$\text{(1)} \qquad U \times [t_1, t_2, \ldots, t_n] = SV \times [t_1, t_2, \ldots, t_n],$$

puisque les termes de S sont au plus égaux à 1 en valeur absolue.

Considérons alors la forme décomposable associée au tableau T,

$$F(x_1, x_2, \ldots, x_n) = \Pi(\omega_i^1 x_1 + \omega_i^2 x_2 + \ldots + \omega_i^n x_n).$$

Les coefficients de F étant des fonctions entières, symétriques séparément par rapport aux conjugués de chaque entier complexe $\omega^{(i)}$, sont des entiers rationnels. Il en est de même pour la forme Φ (équivalente à F) associée au tableau réduit U ou encore au tableau (1). Les termes de ce tableau étant limités supérieurement en valeur absolue, il en est de même des coefficients de Φ et il ne peut y avoir qu'un nombre fini de formes Φ distinctes. Comme la connaissance d'une telle forme n'entraîne celle du tableau auquel elle est associée qu'à une dilatation près, et comme d'autre part, il y a une infinité de tableaux réduits (si $r + s > 1$) équivalents à T, on en déduit que *les tableaux réduits équivalents à T se déduisent tous par des dilatations d'un nombre fini d'entre eux.*

Ceci permet de démontrer qu'*il existe des substitutions automorphes ou semblables de la forme* F. On appelle ainsi toute substitution modulaire Σ qui transforme F en elle-même : ce qui revient à dire qu'au tableau $\Sigma \times T$ est associée la même forme

---

(1) Pour arriver à ce résultat il n'est pas absolument nécessaire de supposer T formé d'entiers, on pourrait encore l'obtenir en remarquant que si T est fractionnaire les normes des termes de $\mathfrak{T}$ sont limitées en valeur absolue.

qu'à T, ou encore que $\Sigma T = TE$, le produit à droite par E étant une dilatation pour T. A chaque substitution automorphe de F correspond une substitution automorphe de Φ. Car, si l'on a $T = SU$, on doit avoir

$$(S^{-1}\Sigma S)U = UE \qquad (S^{-1}\Sigma S \text{ modulaire}).$$

Mais UE est réduit dans le système de tableaux équivalents à TE qui est identique au système défini par T; donc on obtiendra tous les tableaux modulaires $S^{-1}\Sigma S$ en cherchant parmi les tableaux réduits équivalents à T tous ceux qui se déduisent par une dilatation d'un tableau réduit U choisi. La signification des tableaux ainsi trouvés montre que le choix du tableau réduit initial U est indifférent et qu'on doit obtenir les mêmes tableaux Σ, en nombre infini, quel que soit U. Nous allons retrouver directement ces résultats pour un cas plus particulièrement intéressant.

Unités d'un corps.

Supposons pour ce qui va suivre que T soit une base [1] des entiers d'un corps $K(\omega)$ $(r+s>1)$. D'après ce qui précède il y a au moins un tableau U réduit, équivalent à T, tel qu'il existe une infinité de tableaux réduits se déduisant de U par une dilatation, $U' = UE$; *tout tableau canonique* E, *ainsi obtenu, est formé par les conjugués d'un entier du corps dont la norme est* 1 (*c'est-à-dire d'une unité du corps*) *et réciproquement toutes les unités du corps sont ainsi obtenues.*

En effet, U′ étant équivalent à U, on a

$$\Sigma U = UE \qquad \text{ou} \qquad \Sigma = UEU^{-1}.$$

Le tableau Σ ayant pour opérateur une base des entiers de K et étant à termes entiers, son tableau canonique E est bien formé par les n conjugués d'un entier ε complexe de K; en outre,

$$N(\varepsilon) = \Delta(\Sigma) = \pm 1,$$

Réciproquement, si e est une unité de K et si $E = [e_1, e_2, \ldots, e_n]$

---

[1] S'il n'en était pas ainsi, la même recherche conduirait encore aux unités du corps si T était une base d'un idéal du corps ou aux unités *d'un ordre* si T était, à une dilatation près, la base d'un idéal de *l'ordre*.

est le tableau canonique formé par ses n conjugués, le tableau $TET^{-1} = \Sigma$ est unimodulaire. Mais alors, U étant réduit quelconque, UE est un tableau réduit (conditions invariantes pour une dilatation) dans le système de tableaux équivalents à $TE = \Sigma T$ ou encore dans le système défini par T. Comme, pour cette réciproque, on peut supposer que U est un tableau réduit quelconque, on voit que le choix de ce tableau U initial est indifférent.

Nous allons pouvoir déduire de ceci quelques précisions sur la structure de l'ensemble des unités d'un corps. Pour avoir cet ensemble, étant donné un tableau réduit U, il suffit de faire son quotient à droite par chacun des autres tableaux réduits U′ et de conserver ceux de ces quotients qui sont des tableaux canoniques. Il peut se faire d'abord que les termes de U et de U′ soient égaux en valeur absolue, alors les termes de $E = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n]$ ont séparément 1 pour valeur absolue. Remarquons que toute puissance entière d'une unité est encore une unité; dans le cas présent, les valeurs absolues des conjugués de ε^k sont toujours égales à 1. Les points correspondants aux ε^k faisant partie d'un module type et ayant leurs coordonnées limitées supérieurement en valeur absolue sont en nombre fini. Donc les diverses puissances de ε ne sont pas distinctes; on a, par exemple,

$$\varepsilon^{q+r} = \varepsilon^r \qquad \text{ou} \qquad \varepsilon^q = 1;$$

ce qui montre que ε est une racine de l'unité. Il n'existe pas en général de telles unités dans le corps, à l'exception de ± 1; d'après ce que nous avons vu sur les éléments primitifs et imprimitifs, pour que ceci se produise il est nécessaire que le corps soit totalement imaginaire ($2s = n$). En outre, le nombre de ces unités, si elles existent, est fini, leur degré devant être un diviseur de n.

Écartons momentanément ces racines de l'unité, et même ne distinguons pas entre deux unités du corps dont le quotient serait une telle racine. Ceci revient à ne considérer que les valeurs absolues des conjugués de chaque unité. Soit $|e_1|, |e_2|, \ldots, |e_p|$ ces valeurs ($p = r + s$); il y en au moins une différente de 1 d'après notre convention. Posons comme pour les systèmes de paramètres

$$r_1 = \log|e_1|, \qquad r_2 = \log|e_2|, \qquad \ldots, \qquad r_p = \log|e_p|.$$

La condition $N(e) = \pm 1$ entraîne entre les r la relation (4 *ter*)

adoptée pour les paramètres; donc les points $(r_1, r_2, \ldots, r_p)$ appartiennent au sous-espace Λ, ils y constituent un module car le produit ou le quotient de deux unités étant encore une unité, la somme ou la différence de deux tels points appartient encore à l'ensemble. Ce module est type, les inégalités $|r_i| < \varepsilon$ entraînent en effet pour les $|e_i|$ une limitation supérieure et inférieure et il n'y a qu'un nombre fini d'entiers complexes, donc *a fortiori* un nombre fini d'unités satisfaisant à ces conditions.

Enfin ce module est effectivement de dimension $p-1$; considérons un ensemble de tableaux réduits, en nombre fini, dont on peut déduire tous les autres par des dilatations E. Chacun de ces tableaux provient d'un système de minima simultanés A de $\mathfrak{C}$, envisageons dans Λ l'ensemble (¹) $\mathcal{G}$ des points pour lesquels au moins un des A soit minimum; cet ensemble est limité. Si maintenant, nous faisons sur les tableaux réduits précédents une dilatation E, à ces nouveaux tableaux correspond un nouvel ensemble $\mathcal{G}'$ qu'on déduit de $\mathcal{G}$ en remplaçant chaque système de paramètres λ_i par $\frac{\lambda_i}{e_i}$, ou encore, en passant aux logarithmes, chaque point de $\mathcal{G}$,

$$(\rho_1, \rho_2, \ldots, \rho_p), \qquad \text{par} \qquad (\rho_1 - r_1, \rho_2 - r_2, \ldots, \rho_p - r_p);$$

ce qu'on peut traduire géométriquement en disant qu'on fait sur $\mathcal{G}$ la translation $(-r_1, -r_2, \ldots, -r_p)$; tous les ensembles $\mathcal{G}'$ ainsi obtenus doivent couvrir le sous-espace Λ. Or, ceci ne peut se produire si les points $(-r_1, -r_2, \ldots, -r_p)$ appartiennent à un sous-espace de Λ; car s'il en était ainsi, on aurait une relation

$$v_1 r_1 + v_2 r_2 + \ldots + v_p r_p = 0;$$

d'autre part, $\mathcal{G}$ étant limité, ses points vérifient une inégalité de la forme

$$|v_1 \rho_1 + v_2 \rho_2 + \ldots + v_p \rho_p| \leq H',$$

et cette inégalité serait vérifiée par les points de tous les $\mathcal{G}'$ qui ne pourraient donc couvrir Λ (²).

(¹) C'est encore un domaine et en choisissant convenablement les tableaux réduits initiaux, on pourrait s'arranger pour qu'il fût d'un seul tenant et sans trous.

(²) On pourrait modifier la démonstration précédente en montrant, par exemple l'existence d'unités. dont $p-1$ coordonnées seraient inférieures à une quantité donnée, en valeur absolue; la démonstration précédente me paraît plus conforme à l'esprit de la *méthode des variables continues* d'Hermite.

Le module des r étant type et de dimension $p-1$, tous ses points sont donnés par l'égalité

$$\| r_1 \quad r_2 \quad \dots \quad r_p \| = \| x_1 \quad x_2 \quad \dots \quad x_{p-1} \| \times \mathrm{R},$$

les x étant des *entiers* et R une matrice de type $(p-1, p)$ et de rang $p-1$. En remontant des logarithmes aux nombres et en ayant égard à ce que nous n'avons pas distingué entre deux unités différant par une racine de l'unité, on voit que toutes les unités seront comprises dans la formule

$$e = \pm \varepsilon (e^{(1)})^{x_1} (e^{(2)})^{x_2} \dots (e^{(p-1)})^{x_{p-1}},$$

$e^{(i)}$ étant $p-1$ unités convenablement choisies (lignes de R), x_i des exposants entiers et ε les racines de l'unité du corps [2]. On voit en outre que pour $p > 1$ les unités $e^{(i)}$ qu'on peut appeler *fondamentales* ne sont pas déterminées, R n'étant alors défini qu'à une équivalence près : on en déduit immédiatement les relations entre les divers systèmes d'unités fondamentales.

Il n'est pas sans intérêt de constater que, dans chaque cas où l'on aura une méthode pratique de recherche des tableaux réduits, la démonstration précédente donnera non seulement une affirmation d'existence des unités, mais encore un procédé de recherche (on pourrait presque dire le seul procédé de recherche, en tenant compte de la latitude possible dans la définition des tableaux réduits). En précisant dans chaque cas particulier la démonstration du fait que le module est de dimension $p-1$, on trouvera un système d'unités fondamentales (système de translations fondamentales). C'est ainsi que pour le deuxième degré la recherche d'une unité fondamentale est ramenée à un développement en fraction continue.

Indiquons enfin la relation entre ce problème des unités et la résolution d'une certaine équation diophantique. Tout entier complexe a pour conjugués les termes de

$$\| x_1 \quad x_2 \quad \dots \quad x_n \| \times \mathrm{T} \qquad (x \text{ entiers}).$$

---

(1) Dans le cas du deuxième ordre réel ou du troisième ordre à corps imaginaires conjugués, cette formule se réduit à

$$e = \pm (e^{(1)})^{x_1}$$

on peut comparer ceci avec la résolution de l'équation de Pell-Fermat.

Chercher ceux de ces entiers dont la norme est $= \pm 1$ revient à résoudre l'équation diophantique

$$F(x_1, x_2, \ldots, x_n) = \pm 1,$$
$$F = \prod (\omega_i^1 x_1 + \omega_i^2 x_2 + \ldots + \omega_i^n x_n).$$

F est la forme décomposable associée à T (supposé constitué par les entiers $\omega^{(i)}$). Nous avons vu qu'on obtient en même temps les substitutions automorphes de F.

Propriétés du discriminant.

La limitation obtenue pour les termes d'un tableau réduit peut encore s'appliquer à la représentation des termes d'un corps par des tableaux. Toujours avec les mêmes notations que précédemment, le tableau

$$X = U[\varpi_1, \varpi_2, \ldots, \varpi_n]U^{-1}$$

a ses termes rationnels. On peut faire une dilatation sur l'opérateur sans changer X et supposer, en faisant la dilatation $[t_1, t_2, \ldots, t_n]$, que les termes de cet opérateur sont limités supérieurement en fonction de $|\Delta(U)| = |\Delta(T)|$. Il en est de même des termes de X, mais la limite supérieure dépend cette fois de $|\Delta(T)|$ et des valeurs absolues des ϖ_i. Nous allons appliquer ces résultats pour démontrer *qu'il n'y a qu'un nombre fini de corps d'ordre n ayant un discriminant donné d.*

Pour y arriver, supposons qu'on ait représenté les nombres de chaque corps cherché par des tableaux, l'opérateur étant une base réduite U du corps, $|\Delta(U)|$ est égal à $\sqrt{|d|}$. D'après le premier théorème de Minkowski, dans le module de points de base U, existe au moins un point $(\omega_1, \omega_2, \ldots, \omega_n)$ tel que

$$(|\omega_1|, |\omega_2|, \ldots, |\omega_n|) < H|\Delta(U)|;$$

ω est un entier complexe, le tableau correspondant a ses termes entiers et limités supérieurement, en valeur absolue, en fonction seulement de d et H supposés connus. Donc, il ne peut y avoir qu'un nombre fini de tels tableaux, donc de représentations, donc de corps.

Ce théorème a été établi, suivant une marche analogue, par Hermite (*Journal de Crelle*, t. 47), qui l'énonçait : *Il n'y a qu'un nombre fini d'irrationalités distinctes, parmi les racines de toutes les équations algébriques à coefficients entiers de degré et de discriminant donné.* Il entendait par irrationalités non distinctes deux nombres algébriques tels que l'un fût une fonction de l'autre, rationnelle et à coefficients rationnels.

Remarquons encore que la démonstration précédente peut, à la rigueur, constituer une méthode de recherche des corps d'un discriminant donné; toutefois, cette méthode basée sur des inégalités fournirait non seulement les corps dont le discriminant est égal à d, mais ceux pour lesquels il est inférieur (en valeur absolue), et peut-être certains pour lesquels il est supérieur. Enfin, il peut se faire qu'il n'y ait pas de corps dont le discriminant soit d. On peut indiquer à ce propos la propriété trouvée par Minkowski et qui est une conséquence du théorème I : *Le discriminant d'un corps est toujours différent de* ± 1.

En effet, considérons un corps déterminé et T une base de ses entiers; dans le module $\mathfrak{T}$ de base T, on peut trouver un point $A(\alpha_1, \alpha_2, \ldots, \alpha_n)$ et un système de paramètres tel que la spanne à p paramètres $S(OA)$ ne soit pas à la fois de rang $1, 2, \ldots, p$, et soit au plus égal à la racine $n^{\text{ième}}$ de

$$\left(\frac{2}{\pi}\right)^s |\Delta(T)| = \left(\frac{2}{\pi}\right)^s \sqrt{|d|}.$$

On en déduit, α étant l'entier du corps K correspondant à A,

$$|N(\alpha)| = |\alpha_1 \alpha_2 \ldots \alpha_n| < [S(OA)]^n \left[\frac{2}{\pi}\right]^s \sqrt{|d|},$$

ce qui démontre le théorème, puisque $N(\alpha)$ est au moins égal [1] à 1. On peut trouver des limites inférieures plus élevées, en considérant la trace [2] au lieu de la norme, et en supposant alors que S représente l'écart.

---

[1] Dans le cas $n = 2$, $p = 1$, on a $N(\alpha) = |\alpha_1 \alpha_2| = [S(OA)]^2$. Il y a donc exception à la démonstration précédente, mais comme $\left(\frac{2}{\pi}\right)$ est inférieur à 1 la propriété est toujours vraie.

[2] *Voir* sur ce sujet soit la *Geometrie der Zahlen* soit les *Diophantische-Approximationen.*

Classes d'idéaux.

Nous avons vu (Chap. V) qu'en prenant une base d'un idéal entier ou fractionnaire $P \times T$ d'un corps K comme opérateur, on obtient une représentation des entiers complexes de K par des tableaux à termes entiers. A chaque idéal de K correspond ainsi une infinité de représentations en remplaçant $P \times T$ par une base équivalente; on n'en aura plus qu'un nombre fini si l'on convient de ne prendre pour opérateur que des tableaux réduits; en effet, puisque $P \times T$ est une base d'un corps algébrique, ces tableaux réduits se déduisent par dilatation d'un nombre fini d'entre eux, et à deux opérateurs différant par une dilatation correspond une même représentation, nous pouvons dire *que de telles représentations sont réduites.*

Les représentations correspondant à deux idéaux différents $\mathcal{A}$ et $\mathcal{B}$ sont-elles nécessairement distinctes? Pour qu'il y en ait deux confondues, il faut qu'une certaine base de $\mathcal{A}$ se déduise d'une base de $\mathcal{B}$ par une dilatation, $PT = P'T \times [\varpi_1, \ldots, \varpi_n]$; cette dilatation est nécessairement formée par les n conjugués d'un nombre ϖ du corps, non nécessairement entier, de sorte que l'idéal $\mathcal{A}$ doit être égal au produit de $\mathcal{B}$ par l'idéal principal $[\varpi]$

$$\mathcal{A} = \mathcal{B}[\varpi]. \tag{2}$$

Si réciproquement il en est ainsi, à toute base de $\mathcal{A}$ correspond une base de $\mathcal{B}$ déduite par la dilatation $[\varpi_1, \ldots, \varpi_n]$ et inversement, de sorte que toutes les représentations correspondant à $\mathcal{A}$ et $\mathcal{B}$ sont identiques et, en particulier, les représentations réduites (puisqu'elles sont invariantes pour une dilatation)

Nous dirons *que deux tels idéaux dont le quotient est un idéal principal sont équivalents* [1], *et nous noterons*

$$\mathcal{A} \sim \mathcal{B}.$$

Le fait de l'identité des représentations prouve immédiatement que l'équivalence de deux idéaux est réciproque et que deux

---

[1] La raison de cette dénomination est qu'aux bases des idéaux équivalents sont associées des formes décomposables équivalentes, à un facteur numérique près pour leurs coefficients.

idéaux équivalents à un autre le sont entre eux. Ceci résulte aussi des calculs manifestes

$$\mathcal{A} = \mathcal{B}[\varpi], \quad \text{entraîne} \quad \mathcal{B} = \mathcal{A}\left[\frac{1}{\varpi}\right];$$

$$\left.\begin{array}{l}\mathcal{B} = \mathcal{C}[\varpi'],\\ \mathcal{A} = \mathcal{C}[\varpi],\end{array}\right. \quad \text{entraînent} \quad \mathcal{A} = \mathcal{B}\left[\frac{\varpi}{\varpi'}\right].$$

Donc, on peut répartir sans ambiguïté les idéaux *en classes*, deux idéaux d'une même classe étant équivalents. A tous les idéaux d'une même classe correspondent les mêmes représentations réduites en nombre fini. *Tous les idéaux équivalents à* $[1]$ *sont tous les idéaux principaux et forment la classe dite principale.*

Pour chercher si deux idéaux $\mathcal{A}'$ et $\mathcal{A}''$ sont de même classe, considérons l'ensemble des bases réduites de $\mathcal{A}'$, U'_1, U'_2, ...; dans chacune d'elles, divisons les termes des différentes lignes par les termes correspondants de la première ligne, on obtient ainsi des tableaux W'_1, W'_2, ... Pour deux U' différant par une dilatation, les rapports mutuels des termes d'une colonne sont les mêmes, il leur correspond le même tableau W'; donc ces derniers sont en nombre fini. Il suffit de faire les mêmes opérations sur $\mathcal{A}''$, si les U'' diffèrent des U' par une dilatation, les W'' devront être identiques aux W'.

On peut considérer que ces tableaux W' sont caractéristiques d'une classe d'idéaux. Chacun d'eux W' est déduit d'une base U' d'un idéal $\mathcal{A}'$ par une dilatation $\left[\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_n}\right]$; α étant le nombre qui constitue la première ligne de U', donc W' est une base de l'idéal $\mathcal{A}' \times \left[\frac{1}{\alpha}\right]$; on obtient ainsi dans la classe un certain nombre fini d'idéaux $\mathcal{P}$ *qu'on peut appeler encore réduits*, et pour chercher toutes les classes, il suffit de chercher tous ces idéaux réduits; chacun d'eux peut d'ailleurs avoir plusieurs bases réduites. Un tel idéal contient 1, c'est donc l'inverse d'un idéal entier (Chap. V) et sa base relative est l'inverse P^{-1} d'un Tableau à termes entiers.

Nous allons alors montrer que *le nombre des classes d'idéaux est fini*. En effet, tout tableau W' étant réduit dans le système défini par $P^{-1} \times T$, la norme de la première ligne qui est 1 est

inférieure à m_1 ; donc, d'après le premier théorème de Minkowski

$$1 \leq H|\Delta(T)| \cdot |\Delta(P^{-1})|,$$
$$|\Delta(P)| \leq H|\Delta(T)|;$$

$|\Delta(P)|$ est limité supérieurement. Il en est de même des dénominateurs des termes de P^{-1} et le déterminant $\Delta(P^{-1})$ ne peut prendre qu'un nombre limité de valeurs; les tableaux P^{-1} ne peuvent donc appartenir qu'à un nombre fini de systèmes. Mais à des tableaux P^{-1} équivalents correspond un même idéal, il n'y a par conséquent qu'un nombre fini d'idéaux réduits ([1]), donc de classes.

L'équivalence des idéaux est liée à leurs règles de calcul;

$$\begin{aligned} \mathfrak{A} &\sim \mathfrak{B}, \\ \mathfrak{A}' &\sim \mathfrak{B}', \end{aligned} \quad \text{entraînent} \quad \mathfrak{A}\mathfrak{A}' \sim \mathfrak{B}\mathfrak{B}'.$$

En effet, les deux premières égalités traduisent des égalités $\mathfrak{A} = \mathfrak{A}'[\varpi]$, $\mathfrak{B} = \mathfrak{B}'[\varpi']$; on en déduit $\mathfrak{A}\mathfrak{B} = \mathfrak{A}'\mathfrak{B}'[\varpi\varpi']$. On peut encore énoncer ce résultat en définissant le *produit de deux classes d'idéaux;* étant données deux telles classes $\mathfrak{A}$ et $\mathfrak{B}$, on appelle ainsi *la classe* $\mathfrak{C} = \mathfrak{A} \times \mathfrak{B}$ *constituée par tous les idéaux produits d'un idéal de* $\mathfrak{A}$ *par un idéal de* $\mathfrak{B}$. L'ensemble de ces produits est bien une classe d'après ce qui précède; en outre, l'opération ainsi définie est manifestement univoque, associative et commutative, ainsi que la multiplication des idéaux qui sert à la définir. La classe principale $\mathfrak{D}$ joue le rôle de l'unité, car elle est telle que $\mathfrak{D}\mathfrak{A} = \mathfrak{A}$.

Il y a une et une seule classe inverse d'une classe donnée constituée par les inverses des idéaux de la classe primitive, car toutes

---

([1]) On aurait encore pu montrer qu'il n'y a qu'un nombre fini de représentations ayant pour opérateur un tableau W' (*voir* propriétés du discriminant); $|\Delta(W')|$ n'est pas connu, mais limité supérieurement et inférieurement. Donc les termes de

$$W' \times [\omega_1, \ldots, \omega_n] \times W'^{-1}$$

qui sont des entiers rationnels sont aussi limités supérieurement en valeur absolue, quand ω est un entier déterminé du corps

L'inconvénient de cette méthode est de fournir les représentations réduites qui peuvent être en plus grand nombre que les idéaux réduits. Le calcul effectif du nombre de classes est un problème assez difficile et n'a été abordé jusque maintenant que par des méthodes analytiques analogues à celles employées pour la densité des nombres premiers.

les solutions de

$$\mathcal{A}\mathcal{X} \sim [1] \qquad \text{ou} \qquad \mathcal{A}\mathcal{X} = [\varpi],$$

sont données par

$$\mathcal{X} = \mathcal{A}^{-1}[\varpi] \qquad \text{ou} \qquad \mathcal{X} \sim \mathcal{A}^{-1}.$$

On en déduit aisément les règles de calcul [1] sur les classes. Ces classes, étant en nombre fini, forment un groupe d'un nombre fini d'éléments dont la structure est en quelque sorte caractéristique du corps considéré; on pourra aisément la trouver en choisissant un idéal dans chaque classe et en formant leurs produits deux à deux. Cette structure étant établie, tout calcul sur des idéaux se ramènera ensuite à des calculs sur des idéaux principaux, quotients des idéaux donnés par ceux qui servent à représenter les classes.

Remarquons encore que le nombre de classes d'idéaux étant fini, les puissances de l'une d'elles, quelconque, ne sont pas indéfiniment distinctes, c'est-à-dire

$$\mathfrak{A}^{h+g} = \mathfrak{A}^{g} \qquad \text{ou} \qquad \mathfrak{A}^{h} = \mathfrak{O},$$

c'est dire encore que pour tout idéal $\mathcal{A}$ il existe une puissance h telle que $\mathcal{A}^h$ soit principal. Ceci posé, considérons l'ensemble de tous les entiers complexes algébriques et soit α, β, ..., un nombre fini d'entre eux. Ils définissent un corps $K(\alpha, \beta, \ldots)$, et dans ce corps, un idéal entier $\mathcal{A}$ dont une puissance h est un idéal principal $[\omega]$ nécessairement entier; considérons l'entier δ défini, au produit près par une racine de l'unité, par l'équation

$$\delta^h = \omega;$$

Tout entier complexe ξ diviseur commun de α, β, ... divise tous les entiers de $\mathcal{A}$; ξ^h divise les entiers de $\mathcal{A}^h$, et par consé-

(1) Si l'on considère les systèmes de formes décomposables définis respectivement par $\mathfrak{A}$ et $\mathfrak{B}$, le système de formes défini par $\mathfrak{C}$ est tel que chacune de ses formes a pour valeurs numériques les produits des valeurs numériques des premières formes. Un exemple connu de cette composition de deux formes est donné par l'exemple du corps $K(i)$, il n'y a alors qu'une seule classe d'idéaux, la classe principale, les formes décomposables associées ayant pour valeurs numériques des sommes de deux carrés de nombres entiers, ceci se traduit par le fait que le produit d'une somme de deux carrés (d'entiers ordinaires) est une somme de deux carrés.

quent ω, donc ξ divise δ. Réciproquement, δ^h divisant α^h, β^h, ... (quotients entiers algébriques), δ divise α, β, ..., donc, *a fortiori*, tout diviseur de δ divise α, β, ..., c'est dire *que l'ensemble de tous les entiers complexes diviseurs communs de plusieurs entiers en nombre fini* α, β, γ *est identique à l'ensemble de tous les diviseurs d'un même entier complexe* δ (qui n'est pas nécessairement du corps défini par les premiers). C'est l'extension de la propriété du plus grand commun diviseur à l'ensemble (¹) des nombres entiers algébriques.

(¹) Cette propriété, due à M. Dedekind termine un article du géomètre allemand sur les idéaux dans le *Bulletin des Sciences mathématiques* (1879). C'est, à ma connaissance, exception faite de quelques traductions récentes et d'un opuscule de H. Laurent, le seul exposé écrit en français sur l'arithmétique des corps algébriques.



NOTE I.

PÉRIODES DES FONCTIONS.

La théorie des modules est susceptible d'applications intéressantes aux propriétés des fonctions périodiques. Nous allons dans cette Note en indiquer quelques-unes des plus essentielles; la plupart d'entre elles ainsi que les définitions adoptées ont été empruntées au très intéressant Mémoire de M. Esclangon sur les *fonctions quasi-périodiques* (¹).

Nous compléterons d'abord un résultat obtenu pour les modules non types de dimension 1 :

1. *Si un module $\mathfrak{M}$ dans un espace à n dimensions n'est pas type, il existe un sous-module $\mathfrak{L}$ de $\mathfrak{M}$, peut-être confondu avec $\mathfrak{M}$, dont les points forment un ensemble partout dense dans l'espace ou dans le sous-espace de dimension p, qu'ils définissent. En outre, le module $\mathfrak{M}$ se déduit de $\mathfrak{L}$ en ajoutant à chacun de ses points ceux d'un module type $\mathfrak{Q}$ au plus de dimension $n-p=q$.*

En effet il y a une infinité de points de $\mathfrak{M}$ vérifiant

$$(1)\qquad |u_1| < \varepsilon, \qquad |u_2| < \varepsilon, \qquad \ldots, \qquad |u_n| < \varepsilon.$$

quel que soit ε. Pour une première valeur de ε, les solutions définissent un sous-espace linéaire E passant par l'origine et peut-être confondu avec l'espace; si l'on donne à ε des valeurs décroissantes, on obtient des sous-espaces E′, E″, ..., chacun d'eux inclus ou identique au précédent et tous de dimension non nulle. Pour une valeur ε_p suffisamment petite, on obtiendra un sous-espace E_p de dimension p ($m \geq p \geq 1$) qui restera le même pour toutes les valeurs inférieures de ε. C'est dire encore que, pour $\varepsilon < \varepsilon_p$, toutes les solutions de (1) seront dans E_p et qu'on pourra toujours trouver p d'entre elles formant une matrice de rang p.

Soit une telle matrice B dont les valeurs absolues des termes soient inférieures à η et considérons les coordonnées relatives u_i des points

(¹) *Annales de l'Observatoire de Bordeaux*, 1904.

de E_p par rapport à B

$$\| x_1 \quad \dots \quad x_n \| = \| u_1 \quad \dots \quad u_p \| \times B.$$

Alors, si l'on prend un point M déterminé $(u_1, \dots, u_p)$ de E_p, il existe un système d'entiers $(e_1, \dots, e_p)$, tels que

$$(|u_1 - e_1|, |u_2 - e_2|, \dots, |u_p - e_p|) < \frac{1}{2}.$$

Mais ces entiers sont les coordonnées relatives d'un point A de $\mathfrak{M}$ appartenant à E_p, et si a_i en sont les coordonnées absolues et x_i celles de M, les inégalités précédentes entraînent

$$(|x_1 - a_1|, |x_2 - a_2|, \dots, |x_n - a_n|) < \frac{1}{2} p r_i,$$

ce qui montre qu'au voisinage de tout point M de E_p existent des points de $\mathfrak{M}$.

Soit alors P une matrice de ce sous-espace, Q une matrice formant avec P un Tableau d'ordre n, $A = \begin{pmatrix} Q \\ P \end{pmatrix}$ et faisons le changement de coordonnées

$$\begin{aligned} \| x_1 \quad \dots \quad x_n \| &= \| y_1 \quad \dots \quad y_q \quad z_1 \quad \dots \quad z_p \| \times A \\ &= \| y_1 \quad \dots \quad y_q \| \times Q + \| z_1 \quad \dots \quad z_p \| \times P. \end{aligned}$$

Les inégalités (1) entraînent des inégalités analogues pour les nouvelles coordonnées

$$|b_1| < \varepsilon', \quad \dots, \quad |b_q| < \varepsilon'; \quad |c_1| < \varepsilon', \quad \dots, \quad |c_p| < \varepsilon'.$$

Pour les valeurs assez petites de ε', tous les points vérifiant ces inégalités sont dans E_p, c'est-à-dire que les coordonnés b sont toutes nulles; or les points $(b_1, \dots, b_q)$ forment un module, pour ε' assez petit il n'y a aucun de ces points vérifiant les q premières égalités précédentes; donc, quel que soit ε', il n'y en a qu'un nombre fini et le module est type, ou encore

$$\| b_1 \quad \dots \quad b_q \| = \| e_1 \quad \dots \quad e_r \| \times R,$$

R tableau d'ordre $r \leqq q$ et les e entiers. En revenant aux coordonnées absolues des points de $\mathfrak{M}$

$$(2) \qquad \| a_1 \quad \dots \quad a_n \| = \| e_1 \quad \dots \quad e_r \| \times R \times Q + \| c_1 \quad \dots \quad c_p \| \times P.$$

La première partie de la somme du deuxième membre représente des points d'un module type $\mathfrak{Q}$ de dimension $r \leqq q$; la deuxième partie

représente des points d'un module, contenus dans E_p et qui y forment, d'après ce qui a été dit, un ensemble partout dense.

Il y a également intérêt à connaître un criterium pour distinguer le cas des modules denses ou non denses dans tout l'espace :

2. *Pour qu'un module de points* $(a_1, a_2, \ldots, a_n)$ *ne soit pas dense dans tout l'espace, il faut et il suffit qu'on puisse trouver* $u_1, u_2, \ldots, u_n$ *tels que le module de nombres* $(u_1 a_1 + u_2 a_2 + \ldots + u_n a_n)$ *soit type.* C'est dire encore qu'on peut projeter le module sur une droite de façon que le module obtenu soit type.

Si le module est non dense dans tout l'espace, ses points sont donnés par la formule (2) où p, rang de P, est inférieur à n ; alors il suffit de choisir pour les u les coefficients de la première ligne dans le développement du déterminant de $\begin{pmatrix} \mathrm{RQ} \\ \mathrm{P} \end{pmatrix} = \mathrm{A}'$ de façon que

$$\mathrm{RQ} \times \begin{Vmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_n \end{Vmatrix} = \begin{Vmatrix} \Delta(\mathrm{A}') \\ 0 \\ \cdots \\ 0 \end{Vmatrix}, \qquad \mathrm{P} \times \begin{Vmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_n \end{Vmatrix} = \begin{Vmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{Vmatrix}.$$

$$u_1 a_1 + \ldots + u_n a_n = \| a_1 \quad \ldots \quad a_n \| \times \begin{Vmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_n \end{Vmatrix} = e_1 \Delta(\mathrm{A}').$$

Réciproquement si

$$u_1 a_1 + \ldots + u_n a_n = e_1 \alpha,$$

e_i entier quelconque et α déterminé, il n'y a aucun point du module au voisinage d'un point $(x_1, \ldots, x_n)$ tel que

$$u_1 x_1 + \ldots + u_n x_n = \frac{\alpha}{2},$$

et le module n'est pas dense dans tout l'espace.

Fonctions périodiques. — Considérons maintenant une fonction de n variables réelles $F(x_1, x_2, \ldots, x_n)$ supposée définie pour toutes valeurs des x, ou encore dans tout l'espace réel à n dimensions. On dit que cette fonction est *périodique* et admet la période $(a_1, a_2, \ldots, a_n)$ ou plus simplement (a_i) si, quelles que soient les variables x,

$$F(x_1 + a_1, \ldots, x_n + a_n) = F(x_1, \ldots, x_n);$$

on en déduit que, quels que soient les x'_i ($x'_i = x_i + a_i$),

$$F(x'_i - a_i) = F(x'_i),$$

c'est-à-dire que F admet la période $(-a_i)$. Si une fonction admet les deux périodes (a_i), (b_i), elle admet manifestement $(\pm a_i \pm b_i)$; car

$$F(x_i \pm a_i \pm b_i) = F(x_i \pm a_i) = F(x_i).$$

Donc, si l'on considère une période comme définissant un point d'un espace à n dimensions, *les périodes d'une même fonction forment un module.*

Si l'on fait sur les variables x une substitution linéaire définie par

$$\| x_1 \quad \ldots \quad x_n \| = \| y_1 \quad \ldots \quad y_n \| \times A, \qquad \Delta(A) \neq 0,$$

la fonction des x devient une fonction Φ des y encore périodique, dont les périodes (b_i) sont données en fonction des (a_i) par la même substitution. Il peut se faire que, par un choix convenable de A, la fonction Φ ne dépende plus que de q variables au lieu de n, par exemple $y_1, \ldots, y_q$. C'est dire que Φ ou F reste constante lorsque $y_{q+1}, \ldots, y_n$ varient d'une façon quelconque, donc certaines périodes de Φ seront constituées par

$$(0, \ldots, 0, \lambda_{q+1}, \ldots, \lambda_n),$$

les λ ayant des valeurs complètement arbitraires. On en déduit pour F des périodes correspondantes qui seront constituées par tous les points du sous-espace défini par l'origine et les $n - q = p$ dernières lignes de A; c'est ce que M. Esclangon appelle des *périodes impropres.*

Dans le cas où F est *continue* dans tout l'espace, on peut préciser la nature du module formé par ses périodes :

3. *On peut alors ramener* F *par une substitution linéaire à n'être qu'une fonction* Φ *de q variables indépendantes* $(q \leqq n)$, *les périodes relatives à cette nouvelle fonction formant un module type dans l'espace à q dimensions.*

Soit $\mathfrak{M}$ le module des périodes; s'il est type l'ensemble des points de $\mathfrak{M}$ n'est dense dans aucun sous-espace, *a fortiori* il ne contient pas de périodes impropres (formées par tous les points d'un sous-espace) et aucune substitution ne peut diminuer le nombre de variables de F; M. Esclangon appelle une telle fonction, *irréductible.*

Si $\mathfrak{M}$ n'est pas type, ses points, c'est-à-dire les périodes de F, sont donnés par l'égalité (2). Appelons $\Phi(y_1, \ldots, y_q, z_1, \ldots, z_p)$ la fonction transformée de F par la substitution associée au Tableau $\Lambda = \begin{pmatrix} Q \\ P \end{pmatrix}$; cette fonction admet les périodes $(c_1, \ldots, c_p)$ qui forment un ensemble dense dans tout le sous-espace à p dimensions. Donc pour toutes valeurs des z, on peut trouver des c tels que, quel que soit ε,

$$|z_1 - c_1| < \varepsilon, \quad |z_2 - c_2| < \varepsilon, \quad \ldots, \quad |z_p - c_p| < \varepsilon.$$

Mais Φ étant continue, pour un système donné de y, on peut à toute valeur donnée de ε' faire correspondre une valeur de ε, donc des c_i, tels que

$$|\Phi(y_1, \ldots, y_q; z_1, \ldots, z_p) - \Phi(y_1, \ldots, y_q; c_1, \ldots, c_p)| < \varepsilon'$$

ou, en tenant compte de la périodicité,

$$|\Phi(y_1, \ldots, y_q; z_1, \ldots, z_p) - \Phi(y_1, \ldots, y_q; 0, \ldots, 0)| < \varepsilon';$$

comme ε' est arbitraire, on en déduit

$$\Phi(y_1, \ldots, y_q; z_1, \ldots, z_p) = \Phi(y_1, \ldots, y_q; 0, \ldots, 0),$$

c'est dire que Φ ne dépend pas des z et l'ensemble des points (c_i) est identique à celui des points de E_p. Les seules périodes de Φ, considéré comme fonction des y, sont $(b_1, \ldots, b_q)$ et elles constituent un module type, ce qui démontre la proposition énoncée.

Si nous revenons aux périodes mêmes de F, on peut mettre leur expression sous la forme

$$\| a_1 \quad \ldots \quad a_n \| = \| e_1 \quad \ldots \quad e_r \| \times R + \| \lambda_1 \quad \ldots \quad \lambda_p \| \times P.$$

les λ sont des indéterminées quelconques et les e des indéterminées entières; la matrice R de type (r, n) et de rang $r (r \leqq n - p)$ est défini à un produit près à gauche par un tableau unimodulaire d'ordre r; la matrice P de type (p, n) et de rang p est défini à un produit près à gauche par un tableau quelconque d'ordre p. Il est à remarquer que la démonstration resterait valable si F avait des discontinuités isolées.

Si une fonction est irréductible, le module de ses périodes est type de dimension au plus n; c'est dire encore qu'il y a au plus n périodes indépendantes, toutes les autres s'en déduisant par addition et soustraction. Dans le cas particulier d'une seule variable, la fonction est constante ou irréductible; dans ce cas, toutes les périodes, si elles existent, sont de la forme $k\alpha$, k indéterminée entière.

On peut encore appliquer le résultat obtenu à une fonction de n

variables imaginaires $(x_1 + i x'_1, \ldots, x_n + i x'_n)$ en la considérant comme fonction des $2n$ variables réelles $(x_1, x'_1, \ldots, x_n, x'_n)$; si elle est irréductible, elle a au plus $2n$ périodes indépendantes, dont on déduit toutes les autres par addition et soustraction. Les parties réelles et imaginaires de ces $2n$ périodes doivent former un tableau d'ordre $2n$ à déterminant non nul. Il faut pour cela qu'il n'existe entre les $2n$ périodes *aucune relation linéaire et homogène à coefficients réels*. Dans le cas $n = 1$, il ne peut y avoir plus de deux périodes et leur quotient ne peut être réel (*cf.* les *Traités sur les fonctions elliptiques*).

Fonctions quasi-périodiques. — Considérons une fonction périodique irréductible $F(x_1, \ldots, x_n)$ à n variables, les périodes $(a_1, a_2, \ldots, a_n)$ formant une module type $\mathfrak{M}$ de dimension n et de base A (*fonctions entièrement périodiques*). Pour connaître la fonction F, il n'est évidemment pas nécessaire de se donner ses valeurs pour tout point de l'espace, mais seulement pour les points intérieurs à ce qu'on pourrait appeler *un parallélipipède des périodes*, c'est-à-dire, par exemple, pour les points dont les coordonnées relatives au tableau A sont comprises entre 0 et 1 ; tout autre point de l'espace se déduit en effet d'un de ceux-là en ajoutant un point du module type (à coordonnées relatives entières). Mais si F est continue, il n'est pas non plus nécessaire de connaître sa valeur pour tout point de ce parallélipipède, mais seulement pour un ensemble de points qui y soit partout dense; on déduira la valeur de F pour les autres points par continuité. Peut-on arriver au même résultat *en se donnant la valeur de* F *en tous les points d'une droite issue de l'origine, mais convenablement choisie?*

Si les points de la droite ont pour coordonnées $(\alpha_1 t, \alpha_2 t, \ldots, \alpha_n t)$, t paramètre variable; de la donnée de F en ces points, on déduit immédiatement sa donnée en tous les points de l'espace

$$(5) \qquad \xi_1 = \alpha_1 t + a_1, \qquad \xi_2 = \alpha_2 t + a_2, \qquad \ldots, \qquad \xi_n = \alpha_n t + a_n,$$

congrus aux points de la droite (*module* $\mathfrak{M}$) *et formant un module* $\mathfrak{R}$. Pour que cette donnée détermine F, supposée continue, il faut et il suffit que l'ensemble de ces derniers points, qui forment un module, soit dense dans tout l'espace (voir *Traité d'Analyse* de M. Baire, *Principe d'extension*). On conçoit alors l'importance du principe :

4. *Pour que tous les points congrus* (*module* $\mathfrak{M}$), *aux points de*

la droite

$$\frac{x_1}{\alpha_1} = \frac{x_2}{\alpha_2} = \ldots = \frac{x_n}{\alpha_n}$$

(c'est-à-dire les points de $\mathcal{R}$) *forment un ensemble dense dans tout l'espace, il faut et il suffit que, si l'on pose*

$$|\alpha_1 \ \ldots \ \alpha_n| = |\beta_1 \ \ldots \ \beta_n| A,$$

il n'y ait aucune relation, linéaire, homogène, à coefficients entiers entre les β.

Les coordonnées relatives des points (3), relativement à A, sont

$$(3\ bis) \quad \eta_1 = \beta_1 t + e_1, \quad \eta_2 = \beta_2 t + e_2, \quad \ldots, \quad \eta_n = \beta_n t + e_n,$$

les e étant des entiers quelconques. S'il existe entre les β une relation linéaire et homogène à coefficients entiers u_i, on a

$$u_1\eta_1 + u_2\eta_2 + \ldots + u_n\eta_n = u_1 e_1 + \ldots + u_n e_n;$$

le module formé par ces nombres, étant composé d'entiers, est type et le module $\mathcal{R}$ n'est pas dense dans tout l'espace. Réciproquement si $\mathcal{R}$ n'est pas dense dans tout l'espace, on doit trouver des v tels que le module de nombres

$$v_1\eta_1 + v_2\eta_2 + \ldots + v_n\eta_n = (v_1 e_1 + \ldots + v_n e_n) + (v_1\beta_1 + \ldots + v_n\beta_n)t$$

soit type (propriété 2). Pour qu'il en soit ainsi il faut déjà que le coefficient de t soit nul; en outre, les nombres $(v_1 e_1 + \ldots + v_n e_n)$ devant être, quels que soient les entiers e, des multiples entiers d'un même nombre α, les v_i sont de la forme $u_i\alpha$, u_i entier et pour ces entiers, on a

$$u_1\beta_1 + \ldots + u_n\beta_n = 0.$$

M. Esclangon et, en même temps que lui, M. Bohl ont considéré le cas particulier d'un module $\mathfrak{M}$ dont la base A est canonique

$$A = |m_1, \ldots, m_n|$$

(fonction pérodique *séparément* par rapport à chaque variable) et la droite $x_1 = x_2 = \ldots = x_n$. La condition précédente est alors identique à l'absence de toute relation linéaire, homogène à coefficients entiers entre les inverses $\frac{1}{m_i}$. Remarquons qu'à un point de vue, pour ainsi dire inverse, si l'on a trouvé une droite passant par l'origine et remplissant les conditions de la propriété 4, on peut, pour la donnée de F,

remplacer cette droite par toute autre droite parallèle $(\alpha_i t + \gamma_i)$, on ne fait ainsi qu'une translation (γ_i) sur le module $\mathcal{R}$.

Enfin, en supposant toujours F continue, la fonction $f(t)$, obtenue en prenant les valeurs de F sur une des droites précédentes n'est pas quelconque. La donnée *a priori* de f entraîne la donnée de F, en des points d'un ensemble dense, il faut et suffit que la fonction ainsi définie pour ce seul ensemble de points soit elle-même continue (*voir* BAIRE, *loc. cit.*). On peut traduire ceci par une condition nécessaire et suffisante pour f :

5. *Pour que $f(t)$ représente les valeurs d'une fonction périodique* $F(x_1, \ldots, x_n)$ *de périodes*

$$\| a_1 \quad \ldots \quad a_n \| = \| e_1 \quad \ldots \quad e_n \| \times \Lambda \qquad (e_i \text{ entiers}),$$

en tous les points d'une droite $(\alpha_1 t, \ldots, \alpha_n t)$ *vérifiant les conditions de la propriété* 4, *il faut et il suffit qu'étant donné t quelconque et un nombre* $\varepsilon > 0$ *on puisse trouver un nombre* ε', *de façon que pour toute valeur t' telle que*

$$\big|\, |\alpha_1(t - t') - a_1|, \ \ldots, \ |\alpha_n(t - t') - a_n| \,\big| < \varepsilon'$$

ou telle encore que $\beta_i(t - t')$ *diffère de nombres entiers de moins de* ε'', *on ait*

$$|f(t') - f(t)| < \varepsilon.$$

Une telle fonction $f(t)$ est appelée par M. Esclangon *quasi-périodique*, on voit qu'elle n'est pas périodique, mais repasse une infinité de fois par des valeurs aussi voisines qu'on voudra d'une quelconque de ses valeurs. Il existe une infinité de telles fonctions attachées à un même module $\mathfrak{M}$ de périodes et à une même droite. L'expression de ces fonctions au moyen d'un certain nombre d'entre elles se rattache plutôt au domaine de l'Analyse. Je renvoie pour cela le lecteur au Mémoire de M. Esclangon; on y trouvera aussi une question d'ordre plus arithmétique mais que le cadre de cet Ouvrage ne me permet pas de développer : la recherche des différents modules de périodes auxquels est attachée une même fonction quasi-périodique.



NOTE II.

EXEMPLE DE CORPS ALGÉBRIQUE.

Nous allons étudier comme exemple de corps algébrique $K(\sqrt{82})$. L'irrationnelle du deuxième degré $\omega = \sqrt{82}$ est un élément primitif du corps, son conjugué étant $\omega' = -\sqrt{82}$; tout nombre du corps est de la forme $\varpi = x + y\omega$, x et y étant rationnels [forme (1) du Chapitre IV]; la norme de ϖ est

$$N(\varpi) = (x + y\sqrt{82})(x - y\sqrt{82}) = x^2 - 82y^2.$$

On peut voir sur ce cas une propriété générale pour tous les corps du deuxième degré : les nombres du corps conjugué $K(\omega')$ appartiennent au corps lui-même. En prenant pour opérateur commun d'une représentation par des tableaux

$$T = \begin{Vmatrix} 1 & 1 \\ \sqrt{82} & -\sqrt{82} \end{Vmatrix},$$

le nombre ϖ est représenté par

$$\begin{Vmatrix} 1 & 1 \\ \omega & \omega' \end{Vmatrix} \times [x + y\omega,\ x + y\omega'] \times \begin{Vmatrix} 1 & 1 \\ \omega & \omega' \end{Vmatrix}^{-1} = \begin{Vmatrix} x & y \\ 82y & x \end{Vmatrix}.$$

Entiers du corps. — L'équation fondamentale de ϖ est, à un produit près par un entier,

$$X^2 - 2xX + x^2 - 82y^2 = 0.$$

Pour que ϖ soit entier complexe il est nécessaire et suffisant que $2x$ et $x^2 - 82y^2$ soient entiers; il faut donc que $4x^2 - 4 \times 82y^2$ soit aussi entier, et par conséquent aussi $4 \times 82 \times y^2$, comme 82 n'a pas de facteur carré il faut que y comme x soit une fraction de dénominateur 2. Donc x et y sont de la forme $\frac{u}{2}$, $\frac{v}{2}$; u, v étant des entiers et l'on doit avoir

$$u^2 - 82v^2 \equiv 0 \pmod{4} \tag{4}$$

ou

$$(4)\qquad u^2 - 2v^2 \equiv 0 \pmod 4;$$

si u et v sont impairs, leurs carrés sont congrus à 1, module 4, et la congruence précédente ne peut être vérifiée. Si u ou v est pair, l'autre l'est également, c'est dire que x et y doivent être entiers. Donc tout entier complexe du corps est de la forme

$$u + v\sqrt{82} \qquad (u, v \text{ entiers}).$$

On verra sans peine comment ce raisonnement s'étend au cas général d'un corps du deuxième degré $K(\sqrt{d})$, d sans facteur carré; il y a lieu de distinguer deux cas, suivant que d est congru ou non à 1 (module 4).

Une base des entiers du corps est constituée précisément par le tableau T pris comme opérateur. Le déterminant du corps est

$$D = \begin{vmatrix} 1 & 1 \\ \sqrt{82} & -\sqrt{82} \end{vmatrix}^2 = 4 \times 82.$$

les tableaux correspondant aux entiers complexes sont, u, v étant des entiers,

$$\begin{Vmatrix} u & v \\ 82v & u \end{Vmatrix} = [u] \times \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} + [v] \times \begin{Vmatrix} 0 & 1 \\ 82 & 0 \end{Vmatrix}$$

Idéaux du corps. — Cherchons la forme générale de la base relative d'un idéal (entier ou fractionnaire) du corps. On peut mettre cette base sous la forme d'Hermite

$$P = \begin{Vmatrix} \dfrac{p'}{d} & 0 \\ \dfrac{a'}{d} & \dfrac{q}{d} \end{Vmatrix} \qquad (0 \leqq a' < p', \ 0 < q);$$

il faut et il suffit que le tableau

$$P \times \begin{Vmatrix} 0 & 1 \\ 82 & 0 \end{Vmatrix} \times P^{-1} = \begin{Vmatrix} -\dfrac{a'}{q} & \dfrac{p'}{q} \\ \dfrac{82q}{p'} - \dfrac{a'^2}{p'q} & \dfrac{a'}{q} \end{Vmatrix}$$

soit à termes entiers; il faut d'abord que a' et p' soient divisibles par q; si a et p sont leurs quotients, il faut en outre que $\dfrac{82 - a^2}{p}$ soit

un entier. Ces conditions suffisent et tous les idéaux ont pour bases relatives

$$P = \begin{bmatrix} \dfrac{q}{d} \end{bmatrix} \cdot \begin{Vmatrix} p & 0 \\ a & 1 \end{Vmatrix} \qquad [82 - a^2 \equiv 0 \pmod{p}].$$

Nous vérifierons plus loin que certains d'entre eux ne sont pas principaux. Pour qu'un idéal soit entier il faut et il suffit que $\dfrac{q}{d}$ soit un entier ordinaire.

Examinons le cas d'idéaux entiers ($d = 1$); pour que l'idéal de base P soit divisible par celui de base P_1, il faut et il suffit que le tableau

$$P \cdot P_1^{-1} = \begin{bmatrix} \dfrac{q}{q_1} \end{bmatrix} \times \begin{Vmatrix} \dfrac{p}{p_1} & 0 \\ \dfrac{a - a_1}{p_1} & 1 \end{Vmatrix}$$

soit à termes entiers. Cette formule permet la recherche des *idéaux premiers*. Cherchons d'abord ceux de la forme $[q]$ ($p = 1$, $a = 0$), il faut qu'on ne puisse trouver p_1, q_1, a_1 sauf $p_1 = 1$, $q_1 = q$ ou 1, tels que

$$q \equiv 0 \pmod{p_1 q_1}, \qquad q a_1 \equiv 0 \pmod{p_1 q_1},$$
$$82 - a_1^2 \equiv 0 \pmod{p_1}.$$

Il faut d'abord que q soit premier, sinon il suffirait de prendre pour q_1 un de ses diviseurs ($p_1 = 1$, $a_1 = 0$). Alors on doit nécessairement prendre $q_1 = 1$ et $p_1 = q$ et il faut et il suffit qu'il n'existe aucun nombre a_1, tel que

$$82 - a_1^2 \equiv 0 \pmod{q},$$

c'est-à-dire que 82 ne doit pas être *résidu quadratique* module q.

Cherchons maintenant les idéaux premiers pour lesquels $p > 1$, on doit avoir $q = 1$, sinon on aurait comme diviseur $[q]$. Il faut en outre que p soit premier, car si p_1 en était un diviseur, l'idéal $\begin{Vmatrix} p_1 & 0 \\ a & 1 \end{Vmatrix}$ diviserait l'idéal considéré. La condition est d'ailleurs suffisante. Donc en résumé deux sortes d'idéaux premiers

$$[q] \qquad \text{si} \qquad 82 \not\equiv x^2 \pmod{q},$$
$$\begin{Vmatrix} p & 0 \\ a & 1 \end{Vmatrix}, \qquad \text{si} \qquad 82 \equiv a^2 \pmod{p},$$

p et q étant premiers. On verra sans peine comment cette recherche s'étendrait au cas d'un corps quadratique quelconque.

Réduction de la base. — Si l'on approfondit un peu la méthode de réduction exposée au Chapitre VI on trouve sans difficulté que, pour qu'un tableau du deuxième ordre à termes réels $\begin{Vmatrix} a & a' \\ b & b' \end{Vmatrix}$, appartienne à la suite des tableaux réduits du système qu'il définit est que

$$\frac{a}{b} > 1, \qquad 0 > \frac{a'}{b'} > -1,$$

en outre tout tableau de la suite se déduit du précédent en multipliant à gauche par $\begin{Vmatrix} 0 & 1 \\ 1 & -q \end{Vmatrix}$, q étant la partie entière de $\frac{a}{b}$. (*Voir* Mémoire cité). On a un premier tableau réduit équivalent à T qui est

$$\begin{Vmatrix} 1 & 1 \\ \sqrt{82}-9 & -\sqrt{82}-9 \end{Vmatrix},$$

on en déduit le tableau suivant

$$\begin{Vmatrix} 0 & 1 \\ 1 & -18 \end{Vmatrix} \times \begin{Vmatrix} 1 & 1 \\ \sqrt{82}-9 & -(\sqrt{82}+9) \end{Vmatrix} = \begin{Vmatrix} \sqrt{82}-9 & -(\sqrt{82}+9) \\ 163-18\sqrt{82} & 163+18\sqrt{82} \end{Vmatrix}$$

qui est égal au premier multiplié par la dilatation

$$[-9+\sqrt{82},\ -9-\sqrt{82}].$$

Donc une unité du corps est $-9+\sqrt{82}$ et toutes les autres en sont, au signe près, des puissances entières, les puissances négatives ne sont autres que les puissances positives de

$$\pm\frac{1}{-9+\sqrt{82}} = \pm(9+\sqrt{82}),$$

on peut donc aussi prendre ce nombre comme unité fondamentale. Le tableau correspondant est $\begin{Vmatrix} 9 & 1 \\ 82 & 9 \end{Vmatrix}$ et toutes les substitutions automorphes de la forme décomposable associée à T

$$x^2 - 82y^2,$$

sont comprises dans la formule

$$\begin{Vmatrix} 9 & 1 \\ 82 & 9 \end{Vmatrix}^{\pm k}.$$

De même les solutions de

$$x^2 - 82y^2 = -1,$$

sont les entiers des premières lignes des tableaux précédents.

Classes d'idéaux. — Considérons une base réduite d'un idéal réduit, elle est de la forme

$$\left\| \begin{matrix} 1 & 1 \\ \frac{a'}{p'} + \frac{q}{p'}\sqrt{82} & \frac{a'}{p'} - \frac{q}{p'}\sqrt{82} \end{matrix} \right\| = \left\| \begin{matrix} 1 & 0 \\ \frac{a'}{p'} & \frac{q}{p'} \end{matrix} \right\| \cdot \left\| \begin{matrix} 1 & 1 \\ \sqrt{82} & -\sqrt{82} \end{matrix} \right\|;$$

pour que ce tableau soit la base d'un idéal il faut et suffit que

$$p' = qp, \qquad a' = aq, \qquad 82 - a^2 \equiv 0 \pmod{p}.$$

D'autre part en exprimant qu'il est réduit, c'est-à-dire qu'il vérifie les conditions indiquées précédemment, on obtient

$$0 < \frac{a}{p} + \frac{1}{p}\sqrt{82} < 1, \qquad -1 > \frac{a}{p} - \frac{1}{p}\sqrt{82}.$$

Il faut pour cela que a soit négatif et qu'on ait

$$0 < \sqrt{82} + a < p, \qquad p < \sqrt{82} - a,$$

ou, en remarquant que a et p sont des entiers

$$-9 \leq a \leq -1, \qquad 10 + a \leq p \leq 9 - a.$$

Il suffit donc pour obtenir toutes les bases réduites de donner à a toutes les valeurs de -9 à -1 et de prendre pour p les diviseurs de $82 - a^2$ qui sont compris entre $10 + a$ et $9 - a$.

Mais les idéaux réduits ainsi obtenus n'appartiennent pas nécessairement à des classes différentes. Pour répartir ces idéaux en classes, considérons un des tableaux réduits trouvés

$$\left\| \begin{matrix} 1 & 1 \\ \frac{a + \sqrt{82}}{p} & \frac{a - \sqrt{82}}{p} \end{matrix} \right\|.$$

et formons les bases réduites des idéaux réduits dans la classe définie par ce tableau. Il suffit d'appliquer la méthode indiquée pour la recherche des unités et de former le tableau consécutif au précédent dans la suite des tableaux réduits du système. Si α est la partie entière

de $\dfrac{p}{a+\sqrt{82}}$; ce tableau suivant est

$$\begin{Vmatrix}0 & 1\\ 1 & -\alpha\end{Vmatrix}\times\begin{Vmatrix}1 & 1\\ \dfrac{a+\sqrt{82}}{p} & \dfrac{a-\sqrt{82}}{p}\end{Vmatrix}=\begin{Vmatrix}\dfrac{a+\sqrt{82}}{p} & \dfrac{a-\sqrt{82}}{p}\\ \dfrac{p-a\alpha-\alpha\sqrt{82}}{p} & \dfrac{p-a\alpha-a\sqrt{82}}{p}\end{Vmatrix}.$$

et l'idéal réduit correspondant a pour base

$$\begin{Vmatrix}1 & 1\\ \dfrac{p-a\alpha-\alpha\sqrt{82}}{a-\sqrt{82}} & \dfrac{p-a\alpha+\alpha\sqrt{82}}{a-\sqrt{82}}\end{Vmatrix}=\begin{Vmatrix}1 & 1\\ \dfrac{-\alpha p_1-a+\sqrt{82}}{p_1} & \dfrac{-\alpha p_1-a-\sqrt{82}}{p_1}\end{Vmatrix},$$

$$pp_1=82-a^2.$$

Cet idéal peut être identique au précédent; sinon en recommençant le même calcul à partir de cet idéal et ainsi de suite, on finit par retrouver l'idéal dont on était parti et l'on obtient aussi tous les idéaux réduits d'une certaine classe. Si, ce faisant, on n'a pas épuisé tous les tableaux trouvés, on recommencera à partir d'un autre et ainsi de suite.

On peut résumer ainsi les calculs

....	9	− 8	− 7	− 6	− 5	− 4	− 3	− 2	− 1
$-a^2$........	1	18	33	46	57	66	73	78	81
$0+a, 9-a$)..	(1, 18)	(2, 17)	(3, 16)	(4, 15)	(5, 14)	(6, 13)	(7, 12)	(8, 11)	(9, 10)
....	1	2, 3, 6, 9	3, 11	»	»	6, 11	»	»	9

Le Tableau $\begin{Vmatrix}1 & 0\\ 9 & 1\end{Vmatrix}$ est identique à son suivant. Pour les autres on a

$_1$...............	2	9	9	2	3	6	11	3	6	3	11	6
....		1	1	8		2	1	5		5	1	2
$_1=-\alpha p_1-a$....	− 8	− 1	− 8	− 8	− 8	− 4	− 7	− 8	− 8	− 7	− 4	− 8
$_2-a_1^2$..........	18	81	18		18	66	33		18	33	66	

il y a donc quatre classes qu'on peut définir par les idéaux de bases relatives

$$\begin{Vmatrix}1 & 0\\ -9 & 1\end{Vmatrix},\quad\begin{Vmatrix}2 & 0\\ -8 & 1\end{Vmatrix},\quad\begin{Vmatrix}3 & 0\\ -8 & 1\end{Vmatrix},\quad\begin{Vmatrix}6 & 0\\ -8 & 1\end{Vmatrix}$$

ou encore, en prenant des bases équivalentes plus simples

$$\begin{Vmatrix}1 & 0\\ 0 & 1\end{Vmatrix},\quad\begin{Vmatrix}2 & 0\\ 0 & 1\end{Vmatrix},\quad\begin{Vmatrix}3 & 0\\ 1 & 1\end{Vmatrix},\quad\begin{Vmatrix}6 & 0\\ 4 & 1\end{Vmatrix}.$$

La première de ces classes est la classe principale, l'existence des autres montre bien la nécessité de l'introduction des idéaux. Dans l'extension de ces calculs aux corps quadratiques quelconques, il est à remarquer qu'ils se simplifieraient pour les corps imaginaires, chaque classe est alors représentée par un seul idéal réduit.

Structure des classes. — Appelons $\mathfrak{D}$, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, les classes précédentes. Calculons $\mathfrak{A}^2$, l'idéal $\mathcal{A}$ qui représente cette classe est définie par $[2, \sqrt{82}]$ et son carré par

$$[4, 2\sqrt{82}, 82] = [2, 2\sqrt{82}] = [2],$$

idéal qui est principal, et $\mathfrak{A}^2 = \mathfrak{D}$. Calculons $\mathfrak{A} \times \mathfrak{B}$, en faisant le produit des idéaux correspondants on trouve

$$[6, 2 - 2\sqrt{82}, 3\sqrt{82}, 82 - \sqrt{82}] = [6, 2 - 2 \times 82, -3 \times 82, 82 - \sqrt{82}]$$
$$= [6, -82 - \sqrt{82}] = [6, -8 - \sqrt{82}],$$

et cet idéal appartient à la classe $\mathfrak{C}$.

Calculons encore $\mathfrak{B}^2$, le carré de l'idéal représentatif est

$$[9, 3 - 3\sqrt{82}, 83 - 2\sqrt{82}] = [9, -80 - \sqrt{82}, 3 \times 83 - 2 \times 3],$$
$$= [9, -80 - \sqrt{82}] = [9, -8 - \sqrt{82}],$$

ce qui est un idéal de $\mathfrak{A}$. On peut alors résumer la structure

$$\mathfrak{B}, \quad \mathfrak{B}^2 = \mathfrak{A}, \quad \mathfrak{B}^3 = \mathfrak{C}, \quad \mathfrak{B}^4 = \mathfrak{D}.$$

Terminons cet exemple en montrant que les propriétés des nombres premiers rationnels ne pouvaient pas se transporter aux nombres premiers complexes du corps. L'idéal $\mathcal{A} = [2, \sqrt{82}]$ est premier, son carré est l'idéal principal [2], cet idéal ayant pour seul facteur $\mathcal{A}$, le nombre correspondant 2 n'est divisible par aucun entier complexe du corps (car l'idéal correspondant devrait diviser $\mathcal{A}$); on pourrait donc considérer 2 comme premier. Considérons d'autre part l'idéal également premier $\mathcal{B} = [3, 1 + \sqrt{82}]$, son carré est un idéal de $\mathfrak{A}$:

$$\mathcal{B}^2 = [9, -8 - \sqrt{82}] = \left[\frac{5 - \sqrt{82}}{2}\right] \times \mathcal{A}.$$

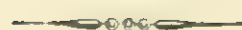
Mais alors l'idéal entier $\mathcal{A}\mathcal{B}^2$ qui appartient à $\mathfrak{A}^2$ est principal

$$\mathcal{A}\mathcal{B}^2 = \left[\frac{5 - \sqrt{82}}{2}\right] \times \mathcal{A}^2 = [10 - \sqrt{82}],$$

il n'a d'autres diviseurs que les idéaux $\mathcal{A}$, $\mathcal{B}$, $\mathcal{A}\mathcal{B}$, $\mathcal{B}^2$ dont aucun n'est principal; le nombre entier complexe $10+\sqrt{82}$ qui n'a aucun diviseur entier complexe pourrait donc être considéré comme premier et notamment comme premier avec 2. *Pourtant le carré de ce nombre*

$$(10+\sqrt{82})^2 = 182+20\sqrt{82}$$

est divisible par 2 (il est contenu en effet dans le carré de l'idéal premier $\mathcal{A}$, qui est 2).



NOTE III.

LES CONGRUENCES SUIVANT UN IDÉAL ET LA NORME D'UN IDÉAL.

Ainsi que nous l'avons fait remarquer à la fin du Chapitre V (p. 90, note 1), il n'existe pas pour les idéaux de notion analogue à celle de la somme ou de la différence de deux nombres. On ne peut donc songer à définir des congruences entre idéaux, mais en revanche on peut définir des *congruences entre nombres d'un corps relativement à un idéal de ce corps*. Il suffit de considérer un idéal entier, comme un sous-module de l'ensemble des entiers du corps et de lui appliquer l'extension toute naturelle faite aux sous-modules, des notions de *congruences et de classes suivant un module entier*, empruntées à l'arithmétique ordinaire. Soit, par exemple, un idéal entier $\mathcal{A}$ de base relative P dans un corps dont la base des entiers est T; on dit que deux entiers complexes, α, β, du corps *sont congrus, module* $\mathcal{A}$,

$$\alpha \equiv \beta \pmod{\mathcal{A}},$$

si α-β est dans $\mathcal{A}$. Les points du module $\mathcal{T}$ (de base T), correspondants à α, β sont, d'après une locution déjà employée (Chap. III, p. 49) congrus suivant le sous-module $\mathcal{A}$ de base $P \times T$. Ces congruences ont les mêmes propriétés que les congruences entre entiers ordinaires :

$$\left.\begin{array}{ll} \alpha \equiv \beta & \pmod{\mathcal{A}} \\ \alpha \equiv \gamma & \pmod{\mathcal{A}} \end{array}\right\} \quad \text{entraînent} \quad \beta \equiv \gamma \pmod{\mathcal{A}},$$

$$\left.\begin{array}{ll} \alpha \equiv \alpha' & \pmod{\mathcal{A}} \\ \beta \equiv \beta' & \pmod{\mathcal{A}} \\ \ldots\ldots & \ldots\ldots\ldots \end{array}\right\} \quad \text{entraînent} \quad f(\alpha, \beta, \ldots) \equiv f(\alpha', \beta', \ldots)$$

f étant une fonction entière à coefficients entiers complexes du

corps. Enfin [1]

$$\left.\begin{array}{ll} \alpha \equiv \beta & (\operatorname{mod} \mathcal{A}) \\ \alpha \equiv \beta & (\operatorname{mod} \mathcal{B}) \\ \ldots & \ldots \end{array}\right\} \text{ entraînent } \alpha \equiv \beta \ (\operatorname{mod} \text{p.p.m.c. } \mathcal{A}, \mathcal{B}, \ldots).$$

Les entiers du corps, ou les points du module $\mathfrak{T}$ associé, peuvent se répartir *en classes* de nombres congrus entre eux suivant l'idéal $\mathcal{A}$, ou suivant le module de points correspondants. D'après le calcul fait au Chapitre III, *le nombre de ces classes est fini et égal à la valeur absolue du déterminant de la base relative de* $\mathcal{A}$, $|\Delta(P)|$; c'est ce qu'on appelle la *norme de* $\mathcal{A}$. Dans le cas d'un idéal principal $[\omega]$, une base est constituée par

$$T \times [\omega_1, \omega_2, \ldots, \omega_n] = P \times T;$$

donc $|\Delta(P)|$ est égal à $|\omega_1 \times \omega_2 \times \ldots \times \omega_n|$, c'est-à-dire que la norme de l'idéal est égale à la valeur absolue de la norme de ω.

On peut étendre cette définition au cas d'un idéal fractionnaire; on appelle *norme* d'un tel idéal la valeur absolue du déterminant de la base relative. On peut encore essayer de relier cette norme (qui est un nombre fractionnaire) à un nombre de classes d'un certain module que le lecteur déterminera aisément. Il est préférable d'en donner ici une autre signification moins immédiate et utile dans beaucoup de cas. *La norme d'un idéal* $\mathcal{A}$, *entier ou fractionnaire, est égale au plus grand commun diviseur des coefficients de la norme d'une forme* $\varphi(x, y, \ldots)$ *contenant* $\mathcal{A}$.

Supposons, par exemple, φ linéaire,

$$\varphi(x, y, \ldots) = x\alpha + y\beta + \ldots,$$

l'idéal $\mathcal{A}$ étant définie par α, β, ..., chacun des tableaux :

$$T \times [\alpha_1, \ldots, \alpha_n], \qquad T \times [\beta_1, \ldots, \beta_n], \qquad \ldots$$

est un tableau du module de points associés à $\mathcal{A}$. Donc

$$\begin{array}{ll} T \times [\alpha_1, \ldots, \alpha_n] = S_\alpha \times P \times T & (S_\alpha \text{ à termes entiers}); \\ T \times [\beta_1, \ldots, \beta_n] = S_\beta \times P \times T & (S_\beta \text{ à termes entiers}); \\ \ldots\ldots\ldots & \ldots\ldots \end{array}$$

---

[1] La première et la troisième propriété sont vraies pour un sous-module quelconque de $\mathfrak{T}$, la deuxième exige que $\mathcal{A}$ soit un idéal. La démonstration résulte du fait évident que la différence $f(\alpha', \beta', \ldots) - f(\alpha, \beta, \ldots)$ est une fonction entière sans terme constant (et à coefficients entiers de $\mathfrak{T}$) des différences $\alpha' - \alpha$, $\beta' - \beta$, ...

et

$$T \times [x\alpha_1 + y\beta_1 + \ldots, \ldots, x\alpha_n + y\beta_n + \ldots] = (xS_\alpha + yS_\beta + \ldots) \times P \times T;$$

d'où, en prenant les déterminants des deux membres

$$\Delta(T) \times \Phi(x, y, \ldots) = \Delta(xS_\alpha + yS_\beta + \ldots) \times \Delta(P) \times \Delta(T);$$

Φ étant la norme de φ, c'est-à-dire le produit des n formes conjuguées $\varphi_1, \varphi_2, \ldots, \varphi_n$ de φ. Soit $\frac{p}{q}$ le plus grand commun diviseur des coefficients de Φ et $\Phi_1 = \frac{p}{q}\Phi$, la forme primaire qu'on en déduit; l'égalité peut s'écrire

$$\frac{1}{\Delta(P)} \frac{p}{q} \Phi_1(x, y, \ldots) = \Delta(xS_\alpha + yS_\beta + \ldots).$$

Le deuxième membre étant une forme linéaire à coefficients entiers, il s'ensuit que $\frac{1}{\Delta(P)} \times \frac{p}{q}$ est un entier rationnel.

Considérons maintenant l'idéal $\mathfrak{A}^{-1}$ inverse de $\mathfrak{A}$ et les idéaux conjugués dans les corps conjugués; ils sont définis respectivement par les coefficients des formes

$$\psi_k(x, y, \ldots) = \frac{1}{\varphi_k(x, y, \ldots)} \frac{q}{p} \Phi(x, y, \ldots).$$

Or, si α' est un de ces coefficients le tableau

$$P \times T \times [\alpha'_1, \alpha'_2, \ldots, \alpha'_n]$$

étant formé par les produits de nombres de $\mathfrak{A}$ par des nombres de $\mathfrak{A}^{-1}$ et leurs conjugués, est formé d'entiers complexes, donc appartient à T. C'est dire que

$$P \times T \times [\alpha'_1, \ldots, \alpha'_n] = U_\alpha \times T \qquad (U_\alpha \text{ à termes entiers});$$
$$P \times T \times [\beta'_1, \ldots, \beta'_n] = U_\beta \times T \qquad (U_\beta \text{ à termes entiers});$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots$$

et

$$P \times T \times [\psi_1, \ldots, \psi_n] = U \times T,$$

U ayant pour termes des fonctions entières à coefficients entiers de $x, y, \ldots$. En prenant les déterminants des deux membres

$$\Delta(P) \times \psi_1 \times \ldots \times \psi_n = \Delta(U),$$

$$\Delta(P)\left(\frac{q}{p}\right)^n \Phi^{n-1}(x, y, \ldots) = \Delta(P)\frac{q}{p}\Phi_1^{n-1}(x, y, \ldots) = \Delta(U).$$

Comme $\Delta(U)$ est une fonction entière à coefficients entiers et Φ_1^{n-1} une fonction primaire, $\Delta(P)\times\frac{q}{p}$ est aussi un nombre entier, ce qui, rapproché de la propriété déjà établie, montre que $\Delta(P)=\pm\frac{p}{q}$. Le théorème est encore vrai pour une forme φ non linéaire.

On déduit de là que le plus grand commun diviseur des coefficients de Φ est indépendant du système de nombres $\alpha, \beta, \ldots,$ servant à définir l'idéal. Réciproquement, si plusieurs nombres $\alpha, \beta, \ldots,$ d'un idéal $\mathcal{A}$ sont tels que le plus grand commun diviseur de la norme de $\alpha x+\beta y+\ldots$ soit égal à la norme de $\mathcal{A}$, ces nombres peuvent servir à définir $\mathcal{A}$, ou encore la forme contient l'idéal. On voit aussi immédiatement qu'un *idéal* $\mathcal{A}$ *contient* tous les coefficients de Φ (norme d'une forme φ contenant $\mathcal{A}$) et par suite leur plus grand commun diviseur qui est *la norme de* $\mathcal{A}$. Si cette norme est 1, $\mathcal{A}$ contenant 1, contient tous les entiers complexes du corps, mais il ne peut contenir de nombres non entiers, sinon φ aurait au moins un tel coefficient α, et Φ ayant au moins un coefficient fractionnaire $[N(\alpha)]$, ne saurait admettre 1 comme plus grand commun diviseur de ses coefficients; donc $\mathcal{A}=[1]$.

Cette même interprétation de la norme fournit encore une démonstration simple de la propriété : *La norme d'un produit d'idéaux* $\mathcal{A}\times\mathcal{A}'$ *est égal au produit des normes.* Soient deux formes

$$\varphi=\alpha x+\beta y+\ldots,\qquad \varphi'=\alpha' x'+\beta' y'+\ldots.$$

contenant respectivement $\mathcal{A}$ et $\mathcal{A}'$; le produit

$$\varphi\times\varphi'=\alpha\alpha' xx'+\alpha\beta' xy'+\beta\alpha' x'y+\ldots$$

est une forme contenant $\mathcal{A}\mathcal{A}'$. Or $\frac{1}{N(\mathcal{A})}\times N(\varphi)$ et $\frac{1}{N(\mathcal{A}')}\times N(\varphi')$ étant deux polynomes primaires, leur produit est aussi primaire, ce qui montre bien que $N(\mathcal{A})\times N(\mathcal{A}')$ est le plus grand commun diviseur des coefficients de la norme de $\varphi\varphi'$, c'est-à-dire est la norme du produit $\mathcal{A}\mathcal{A}'$.

Revenons au cas de $\mathcal{A}$ entier et à la première définition de la norme. Nous supposerons, ce qu'il est toujours possible de réaliser, que la première ligne de T est formée de 1 et que la base relative de $\mathcal{A}$ (à termes entiers) est sous la forme réduite d'Hermite

$$P=\begin{Vmatrix} p & 0 & \ldots & 0 \\ a_2^1 & p_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_n^1 & a_n^2 & \ldots & p_n \end{Vmatrix}.$$

Aux entiers rationnels de $\mathfrak{A}$ correspondent les points du module dont les $n-1$ dernières coordonnées relatives par rapport à T sont nulles. Or p est le plus grand commun diviseur des premières coordonnées de ces points (*voir* Chap. II, la démonstration du théorème fondamental), c'est-à-dire que *p est le plus grand commun diviseur des entiers rationnels de $\mathfrak{A}$*. De même si la deuxième ligne de T est formée des conjugués de l'entier complexe ω, pour tous les nombres de $\mathfrak{A}$ qui sont de la forme $x\omega$, (x entier rationnel) les $n-2$ *dernières* coordonnées relatives par rapport à T sont nulles: ces nombres sont de la forme $yp_2\omega$ (mais non réciproquement). Or l'idéal $\mathfrak{A}$ contient l'entier $p\omega$, *donc p_2 est un diviseur de p; il en est de même de $p_3, \ldots, p_n$.*

Considérons plus particulièrement le cas de $\mathfrak{A}$ *premier;* alors *l'entier p est nécessairement premier* dans le domaine des entiers rationnels. Sinon on aurait

$$p = p' \times p'', \qquad [p] = [p'] \times [p'']:$$

l'idéal premier $\mathfrak{A}$ qui divise $[p]$ diviserait l'un des facteurs $[p']$ ou $[p'']$; c'est-à-dire que $\mathfrak{A}$ devrait contenir l'un des entiers rationnels p' ou p'' qui n'est plus multiple de p. Les nombres $p_2, \ldots, p_n$ sont alors égaux respectivement à 1 ou à p et la *norme de $\mathfrak{A}$ est égale à*

$$p^f \qquad (f \leq n),$$

c'est-à-dire à une puissance du nombre premier, plus grand commun diviseur des nombres rationnels contenus dans $\mathfrak{A}$. Cette puissance f est appelé le *degré de l'idéal* $\mathfrak{A}$.

D'autre part l'idéal $\mathfrak{A}$ contenant p, l'idéal principal $[p]$ est divisible par $\mathfrak{A}$ qui est par suite un des facteurs de la décomposition de $[p]$ en facteurs premiers

$$[p] = \mathfrak{A} \times \mathfrak{B} \times \ldots.$$

Si l'on a égard à l'égalité des normes des deux membres

$$\mathrm{N}([p]) = p^n = \mathrm{N}(\mathfrak{A}) \times \mathrm{N}(\mathfrak{B}) \times \ldots,$$

on voit, d'une part, que les normes de $\mathfrak{A}$, $\mathfrak{B}$, ... sont des puissances de p

$$\mathrm{N}(\mathfrak{A}) = p^{f_1}, \qquad \mathrm{N}(\mathfrak{B}) = p^{f_2}, \qquad \ldots,$$

d'autre part ces facteurs sont au plus en nombre n. On obtient donc la suite des idéaux premiers d'un corps, en considérant la suite des entiers rationnels premiers p et en décomposant dans le corps les

idéaux $[p]$ en produits de facteurs premiers. Comme à des p distincts correspondent des idéaux premiers distincts, il existe bien *une infinité d'idéaux premiers.*

Au sujet de cette recherche des idéaux premiers, on peut se poser deux problèmes sur lesquels je me contenterai de donner ici quelques brèves indications. On peut d'abord chercher les nombres premiers rationnels p dont les facteurs premiers idéaux ne sont pas tous distincts. Ces entiers sont en nombre fini et coïncident avec les diviseurs du discriminant du corps, je renvois pour la démonstration aux travaux de MM. Dedekind et Hensel. Signalons seulement que ces diviseurs, qu'on appelle quelquefois *nombres critiques*, jouent un rôle important dans la constitution de l'arithmétique du corps (notamment dans la structure du groupe formé par les classes d'idéaux, Chap. VII). On peut rapprocher ce rôle de celui joué par les points de ramification (diviseurs de la fonction discriminante) dans l'étude des fonctions algébriques : c'est ce rapprochement qui sert en somme de point de départ lorsqu'on étudie simultanément les corps de nombres et de fonctions. (*Voir* l'*Encyclopédie*, t. I, p. 10, articles de G. Landsberg, de J. Hadamard et J. Kürshàk dans l'édition française; et les travaux de K. Hensel, G. Lanasberg, J. König, etc.)

Ces nombres premiers critiques mis à part, on peut ensuite se proposer de répartir les autres nombres premiers en catégories suivant le nombre et les degrés respectifs de leurs facteurs premiers. Dans la Note précédente, on a pu voir comment cette répartition est liée, dans les corps quadratiques, à la notion de résidus quadratiques (symbole de Legendre); pour les corps de la division du cercle (définis par une racine $m^{\text{ième}}$ de l'unité) elle dépend de l'*exposant auquel appartient p relativement au module m* (dans le cas de m premier). Pour les corps plus généraux cette question se rattache à l'étude de congruences de degré supérieur à 1 relativement à un module entier rationnel, on pourra en trouver un exemple élémentaire (corps du troisième ordre) dans le livre de M. Sommer, traduit par M. Levy. (*Voir* aussi aux *Comptes rendus de l'Académie des Sciences*, séance du 15 mai 1911, une Note sur les corps abéliens du troisième ordre.)

Indiquons enfin comment on peut étendre aux congruences, suivant un idéal, les propriétés classiques de la théorie des nombres ordinaires. Soit donc un idéal premier $\mathfrak{A}$ de norme $p^f = m$; il existe m classes d'entiers complexes du corps, incongrues suivant le module $\mathfrak{A}$; nous désignerons par

$$0, \quad \alpha', \quad \ldots, \quad \alpha^{(m-1)},$$

une suite de représentants de chacune de ces classes, o appartenant à $\mathcal{A}$. Ceci posé, soit a un entier complexe non dans $\mathcal{A}$, ou encore tel que $[a]$ soit premier avec $\mathcal{A}$, et multiplions a successivement par tous les nombres o, $\alpha^{(i)}$; on obtient m nombres incongrus, *mod.* $\mathcal{A}$, et qui, par conséquent, constituent une nouvelle suite de représentants des m classes. Ceci prouve d'abord que l'équation congruentielle

$$a x \equiv b \qquad (\text{mod}\, \mathcal{A})$$

est, quel que soit b, vérifiée par les nombres d'une et d'une seule classe. En outre, si l'on fait le produit des $m-1$ congruences

$$a\alpha' \equiv \beta', \qquad a\alpha'' \equiv \beta'', \qquad \ldots, \qquad a\alpha^{(m-1)} \equiv \beta^{(m-1)};$$

en ayant égard à ce que la suite des β peut être prise, à l'ordre près, identique à celle des α, on obtient

$$a^{m-1} \equiv 1 \qquad (\text{mod}\, \mathcal{A}),$$

quel que soit a, non dans $\mathcal{A}$. C'est l'extension du *théorème de Fermat, la norme de l'idéal remplaçant la valeur absolue du nombre premier*.

D'autre part, si l'on considère la suite des classes auxquelles appartiennent les puissances successives a, a^2, ..., on voit sans peine que cette suite est périodique; si l'on obtient ainsi h classes différentes, on a

$$a^h \equiv 1 \qquad (\text{mod}\, \mathcal{A}),$$
$$a^{\mu+\lambda h} \equiv a^{\mu} \qquad (\text{mod}\, \mathcal{A}):$$

cette deuxième propriété admet sa réciproque. Il s'ensuit que h est un diviseur de $m-1$; c'est, en adoptant la locution classique, *l'exposant auquel appartient a suivant le module* $\mathcal{A}$. Je laisse au lecteur le soin d'étendre de même la notion de racines primitives, le raisonnement si ingénieux de Gauss, pour l'existence de ces racines, et la théorie des indices de Jacobi. On fera aussi aisément l'extension de la fonction $\varphi(m)$ pour un idéal non premier et l'extension à ce cas du théorème de Fermat.

Considérons encore à un autre point de vue une équation congruentielle

$$f(x) \equiv 0 \qquad (\text{mod}\, \mathcal{A}),$$

f étant un polynome et $\mathcal{A}$ un idéal premier. Si elle est vérifiée par un nombre entier α du corps, on a *identiquement* (c'est-à-dire que les coefficients des mêmes puissances sont congrus)

$$f(x) \equiv (x-\alpha) f_1(x) \qquad (\text{mod}\, \mathcal{A}).$$

On en déduit que les solutions distinctes (mod $\mathcal{A}$) sont au plus en nombre p, p étant le degré de f, sauf si tous les coefficients de f sont congrus à o. Mais il peut se faire, si $p \geqq m$, que l'équation soit vérifiée par un nombre de chaque classe, et par suite par tous les entiers du corps, il faut et il suffit pour cela que f soit *divisible, module* $\mathcal{A}$, par

$$x(x-\alpha') \times \ldots \times (x-\alpha^{(m-1)}).$$

D'après le théorème de Fermat, la propriété précédente est vérifiée par $x^m - x$, et comme il y a égalité entre les degrés d'une part et les coefficients de x^m d'autre part, on a l'identité congruentielle

$$x^m - x \equiv x(x-\alpha') \times \ldots \times (x-\alpha^{(m-1)}) \pmod{\mathcal{A}}$$

qui entraîne notamment la congruence

$$\alpha' \times \ldots \times \alpha^{(m-1)} = -1 \pmod{\mathcal{A}}.$$

c'est la généralisation du *théorème de Wilson*. On entrevoit ainsi toute l'importance du théorème de Fermat dans la théorie des équations congruentielles, les conséquences s'en déduiraient comme pour les nombres entiers ordinaires et je renvoie pour ces conséquences aux Traités élémentaires de théorie des nombres, par exemple l'*Algèbre* de Serret. [On en trouvera aussi des applications aux polynomes à plusieurs variables dans quelques articles de M. Borel (*Bulletin des Sciences mathématiques*).]

FIN.

TABLE DES MATIÈRES.

FIN DE LA TABLE DES MATIÈRES.

5176) Paris. — Imp. GAUTHIER-VILLARS, 55, quai des Grands-Augustins.

